Windows Server 2008系统工程师 视频突击



Windows Server 2008 系统管理之道

韩立刚 张 辉 编著

超值赠送 DVD 30小时的Windows Server 2008系统管理视频操作
20小时的Windows Server 2003系统管理视频操作

清华大学出版社

Windows Server 2008 系统工程师视频突击

Windows Server 2008 系统管理之道

韩立刚　张　辉　编　著

清华大学出版社

北　京

内 容 简 介

Windows Server 2008 是微软最新的服务器操作系统，代表了下一代 Windows Server。使用 Windows Server 2008，IT 专业人员对其服务器和网络基础结构的控制能力更强，从而可重点关注关键业务需求。本书以 Windows Server 2008 的管理为重点，其中包括了 Windows Server 2008 在安装方面的改进、Windows Server Core 操作系统的管理、服务器硬件和软件管理、创建和管理用户和组、管理网络凭据、搭建域环境、使用 NTFS 管理数据、配置文件服务器和分布式文件系统、配置服务器系统安全策略、监视和优化系统性能、配置网络打印机、远程桌面和终端服务的使用、Hyper-V 虚拟化技术、动态磁盘管理、热备群集服务、网络负载均衡和 QoS。

本书在各个章节不只是 Windows Server 2008 功能的介绍或简单罗列，各个章节都是先理论、后实战的原则。有实战目标、实战场景、实战中的服务器环境以及在各个服务器上的配置步骤和配置成功后的验证。让读者能够触类旁通，将这些实战中的场景很容易的实施在自己的企业中。

本书光盘是本书的亮点，由资深系统管理专家精心录制的长达 40 小时的 Windows Server 2008 系统管理视频。

本书读者对象：企业 IT 部门系统管理员、想进入 IT 领域的大学生、想考取微软新一代认证 MCITP 的在职人员或在校学生。

图书在版编目(CIP)数据

Windows Server 2008 系统管理之道/韩立刚，张辉编著. —北京：清华大学出版社，2009.11
(Windows Server 2008 系统工程师视频突击)
ISBN 978-7-302-21288-1

Ⅰ. W…　Ⅱ. ①韩…　②张…　Ⅲ. 服务器—操作系统(软件)，Windows Server 2008　Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2009)第 181809 号

责任编辑： 栾大成
装帧设计： 杨玉兰
责任校对： 李玉萍
责任印制：

出版发行： 清华大学出版社　　**地　址：** 北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：** 100084
社 总 机： 010-62770175　　**邮　购：** 010-62786544
投稿与读者服务： 010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈： 010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销： 全国新华书店
开　　本： 210×280　**印　张：** 36.5　**字　数：** 885 千字
附光盘 1 张
版　　次： 2009 年 11 月第 1 版　**印　次：** 2009 年 11 月第 1 次印刷
印　　数： 1~5000
定　　价： 69.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：

前　　言

Windows Server 2008 是微软最新的服务器操作系统，它是 Windows Server 2003 的升级版本。Windows Server 2008 是一套相当于 Windows Vista 的服务器系统，两者拥有很多相同功能；Vista 及 Windows Server 2008 与 Windows XP 及 Windows Server 2003 间存在相似的关系。

Microsoft Windows Server 2008 代表了下一代 Windows Server。通过使用 Windows Server 2008，IT 专业人员对其服务器和网络基础结构的控制能力更强，从而可重点关注关键业务需求。Windows Server 2008 通过加强操作系统和保护网络环境提高了安全性。通过加强对 IT 系统的部署与维护，使服务器和应用程序的合并与虚拟化更加简单；通过提供直观管理工具，Windows Server 2008 还为 IT 专业人员提供了灵活性。Windows Server 2008 为任何组织的服务器和网络基础结构奠定了良好的基础。

Microsoft Windows Server 2008 用于在虚拟化工作负载、支持应用程序和保护网络方面向组织提供了高效的平台。它为开发和可靠地承载 Web 应用程序和服务提供了一个安全、易于管理的平台。从工作组到数据中心，Windows Server 2008 提供了许多有价值的新功能，同时对基本操作系统作了重大改进。

本书以 Windows Server 2008 的管理为重点，其中包括 Windows Server 2008 在安装方面的改进、Windows Server Core 操作系统的管理、服务器硬件和软件管理、创建及管理用户和组、管理网络凭据、搭建域环境、使用 NTFS 管理数据、配置文件服务器和分布式文件系统、配置服务器系统安全策略、监视和优化系统性能、配置网络打印机、远程桌面和终端服务的使用、Hyper-V 虚拟化技术、动态磁盘管理、双机热备群集服务、网络负载均衡和 QoS。

本书不只是 Windows Server 2008 功能的介绍或简单罗列，各个章节都按先理论、后实战的原则，有实战目标，实战场景，实战中的服务器环境，以及在各个服务器上的配置步骤，以及配置成功后的验证，从而让读者能够触类旁通，将这些实战中的场景很容易地实施到自己的企业中。

内容简介

第 1 章　Windows Server 2008 技术概述

从更强的控制能力、增强的保护和更大的灵活性三个角度介绍了 Windows Server 2008 的新增功能。

第 2 章　安装 Windows Server 2008

Windows Server 2008 版本介绍，Windows Server 2008 在安装方面的改进。激活 Windows Server 2008。

第 3 章　配置 Windows Server 2008 环境

本章讲解了 Windows Server 的新概念：角色和功能、管理计算机硬件和软件环境、配置反间谍软件、定义用户桌面环境、配置网络中心以及网络排错工具介绍。

第 4 章　管理本地户和组

我们可以使用 Windows Server 图形界面的管理工具管理 Windows Server Core 上的用户和组。管理访问其他服务器的凭据，管理存储的账户，使用用户账户控制保护系统安全。

第 5 章　Windows Server 2008 活动目录

本章介绍了计算机的两种组织形式：域和工作组。搭建域环境实现计算机和用户的集中管理和用户的集中身份验证。根据管理的需要设计组织单位，介绍在域中使用组的策略。

第 6 章　利用 NTFS 管理数据

NTFS 分区和 FAT32 分区的区别，将 FAT32 分区转化成 NTFS 分区，利用 NTFS 权限控制对数据的访问，利用 EFS 加密数据，在 NTFS 分区上压缩数据，配置 NTFS 分区上的磁盘限额，配置卷影副本。

第 7 章　搭建文件服务器

创建共享和隐含共享，能够访问共享文件夹、隐含共享以及默认共享，使用 DFS 逻辑上整合数据以及实现数据的冗余。安装文件服务角色，控制文件夹存放的数据类型。实现文件夹大小控制。

第 8 章　监视和优化性能

利用日志监控系统出现的错误或警告，使用任务管理器监控计算机内存和 CPU 的使用情况，使用性能计数器监控计算机特定的性能指标，跟踪服务器性能，找到服务器的性能瓶颈。

第 9 章　Windows Server 2008 安全策略

通过配置本地安全策略，可以加固服务器安全。从以下几个方面配置服务器安全：账户策略，审核策略，用户权限分配，安全选项，软件限制策略，高级 Windows 防火墙。

第 10 章　配置打印功能

在打印服务器上添加打印机驱动，共享打印机，设置打印池，打印机优先级，配置打印机使用权限，以及打印作业存放位置，在客户端连接打印服务器共享的打印机。

第 11 章　磁盘管理

利用动态磁盘可以创建条带卷(RAID-0)，镜像卷(RAID-0)以及 RAID-5。其中 RAID-0 和 RAID-5 有容错能力，RAID-0 有很好的读写性能。

第 12 章　终端服务

终端服务和远程桌面区别，在终端服务上配置 RemoteApp，配置终端服务网关，配置 TS Session Broke。

第 13 章　Windows Server 虚拟化

Windows Server 2008 64 位操作系统内置 Hyper-V，安装 Hyper-V，在虚拟机中安装操作系统，创建差异磁盘，创建快照，管理 Hyper-V 的网络。

第 14 章　高可用群集和 QoS

介绍网络负载平衡技术的应用场景，配置网络负载平衡和验证网络负载平衡。在 Windows Server 配置 QoS 策略限制拷贝文件占用的网络带宽。

第 15 章　故障转移群集

本章内容包括：安装和配置虚拟存储，配置 Windows Server 2008 使用 iSCSI，配置心跳线，安装故障转移群集，确定仲裁磁盘，配置文件服务器双节点群集。

致谢

任何一本书的出版，都离不开身边的家人、朋友等的关心和帮助。以下诸位都为本书提供了极大帮助。河北师范大学的蒋春澜教授、邓明利教授为作者创造了优越的写作条件与实验环境。河北师范大学的赵书良教授、河北经贸大学的王顶老师等对本书的组织、行文提出了许多好的建议。

感谢河北师范大学软件学院的全体教师，他们中的大多数人阅读了本书初稿，指出了书中的不少错误，并配合录制了本书视频。

在书稿编辑方面，来自清华大学出版社的栾大成先生给予了很大帮助，对他们的敬业表示敬意，对他们为本书出版所做的一切工作表示深深感谢。应该说，与清华大学出版社的合作是一件令人愉悦的事情。

需要特别感谢的是河北师范大学软件学院的管理层，他们开明的态度和鼎力支持使作者能有充分的时间和空间写作本书，包括：罗忠华先生、赵胜老师等。

首先特别感谢我的家人，感谢父母对我的支持和鼓励；感谢妻子的大力支持，才使得我有时间、有精力去完成本书的编写。感谢河北师大软件学院的领导李文斌博士的大力支持，同时感谢并肩进行写作的张辉，尤其要感谢编辑 Mr.栾的大力支持。希望各位读者在收获知识的同时不吝批评指正。

——韩立刚

MSN：onesthan@hotmail.com

感谢家人的支持，感谢读者朋友的选择，特别要感谢共同完成写作的“战友”，对 Microsoft 新技术的狂热让我们走到一起，携手奋斗。希望带给读者朋友更多的收获。

——张辉

MSN：superergou@hotmail.com

目　　录

第 1 章　Windows Server 2008 技术概述

Windows Server 2008 可以在虚拟化工作负载、支持应用程序和保护网络方面向组织提供高效的平台。它为开发和可靠地承载 Web 应用程序和服务提供了一个安全、易于管理的平台。从工作组到数据中心，Windows Server 2008 提供了许多很有价值的新功能，同时对基本操作系统作了重大改进。本章将从以下三个角度介绍 Windows Server 2008 的新功能。

- 更强的控制能力。通过使用 Windows Server 2008，IT 专业人员能够更好地控制服务器和网络基础结构，从而可将精力集中在处理关键业务需求上。
- 增强的保护。Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。
- 更大的灵活性。Windows Server 2008 的设计允许管理员修改其基础结构以适应不断变化的业务需求，同时保持了此操作的灵活性。

关键词

- 简介
- 虚拟化
- Web 和应用平台
- 服务器管理
- 服务器核心
- Windows Server 2008 打印管理
- 安全和策略实施
- 集中式应用程序访问
- 对分支机构的支持
- 高可用

1.1 概　　述

图 1-1 显示了 Windows Server 2008 的新特性。



图 1-1　Windows Server 2008 新增功能

1. 更强的控制

通过使用 Windows Server 2008，IT 专业人员能够更好地控制服务器和网络基础结构，从而可将精力集中在处理关键业务需求上。其增强的脚本编写功能和任务自动化功能(例如，Windows PowerShell)可帮助 IT 专业人员自动执行常见任务。通过服务器管理器进行的基于角色的安装和管理简化了在企业中管理与保护多个服务器角色的任务。服务器的配置和系统信息是通过新的服务器管理器控制台这一集中位置来管理的。IT 人员可以仅安装需要的角色和功能，向导会自动完成许多费时的系统部署任务。增强的系统管理工具(例如，性能和可靠性监视器)可提供有关系统的信息，从而在潜在问题发生之前向 IT 人员发出警告。

2. 增强的保护

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。Windows Server 2008 提供了减小内核攻击面的安全创新(例如 Patch Guard)，从而使服务器环境更安全、更稳定。通过保护关键服务器服务使之免受文件系统、注册表或网络中异常活动的影响，Windows 服务强化有助于提高系统的安全性。借助网络访问保护(NAP)、只读域控制器(RODC)、公钥基础结构(PKI)增强功能、Windows 服务强化、新的双向 Windows 防火墙和新一代加密支持，Windows Server 2008 操作系统中的安全性也得到了增强。

3. 更大的灵活性

Windows Server 2008 的设计允许管理员修改其基础结构以适应不断变化的业务需求，同时保持了此操作的灵活性。它允许用户从远程位置(如远程应用程序和终端服务网关)执行程序，这一技术为移动工作人员增强了灵活性。Windows Server 2008 使用 Windows 部署服务(WDS)加速对 IT 系统的部署和维护，使用 Windows Server 虚拟化(WSv)帮助合并服务器。对于需要在分支机构中使用域控制器的组织，Windows Server 2008 提供了一个新配置选项：只读域控制器(RODC)，它可以防止在域控制器出现安全问题时暴露用户账户。

1.2 虚 拟 化

图 1-2 显示了微软完整的虚拟化解决方案。



图 1-2 Microsoft 完整的虚拟化解决方案

Windows Server 2008 系列包括 Windows Server 虚拟化(WSv)，这是一项强大的虚拟化技术，具有强大的管理功能和安全功能。通过 WSv，企业可以利用已掌握的 Windows 服务器管理技能，而无须购买第三方软件即可享有虚拟化的灵活性和安全性方面的好处。Microsoft 及其合作伙伴为 Windows 及受支持的 Linux 来宾操作系统提供了全面的支持。WSv 是一个高灵活性、高性能、经济高效且广受支持的虚拟化平台。

Microsoft Windows Server 虚拟化包括解决许多高难度虚拟化挑战的功能，其中包括：确保合并服务器的安全、响应动态工作负载、实现高性能和可伸缩性以便虚拟化工作负载及简化管理。WSv 同时提供安全性和强大的 VM 隔离功能，从而可以在 WSv 主机服务器上合并异类工作负载，且保持灵活性和安全性。构成 WSv 基础的 64 位管理程序体系结构为要求较高的工作负载提供了高性能。Windows Server 2008 中强大的集成管理功能、System Center Operations Manager(系统中心操作管理器)和 System Center Virtual Machine Manager(系统中心虚拟机管理器)支持在广泛的虚拟化环境中实现自动而高效的控制。

1.2.1 安全

安全在任何服务器实现过程中都是一项核心挑战。承载多台虚拟机(VM)的服务器(也称为合并服务器)不仅要承担与非合并服务器同样的安全风险，还要面对管理员角色分离的挑战。WSv 有助于提高合并服务器的安全性和解决管理员角色分离的挑战。WSv 通过下列功能来实现此目的。

- 强大的分区能力：虚拟机(VM)就如同完全独立于运行在同一物理服务器上的其他虚拟机的独立操作系统容器。
- 硬件级别安全性：较新的服务器硬件中提供了数据执行保护(DEP)之类的功能，这有助于阻止大多数流行病毒和蠕虫的执行。
- Windows Server 虚拟化：WSv 可防止暴露包含敏感信息的 VM，还可保护基本主机操作系统不

会因来宾操作系统而降低安全性。

- 网络安全功能：启用了自动网络地址转换(Network Address Translation，NAT)、防火墙和网络访问保护(Network Address Protection，NAP)。
- 最小的受信任计算基础：减少了攻击面并提供简化的轻型虚拟化体系结构。此功能可增强基于 WSv 虚拟机的可靠性。

在某些情况下，配置为每个应用程序提供最佳安全性和操作系统环境的合并服务器可能面临严峻的挑战。由于 WSv 创建了一个环境，在其中可以对每个工作负载配置理想的操作系统环境和安全配置文件，所以 WSv 解决了合并服务器上的角色分离问题。WSv 允许 VM 在仅具有所需权限的服务账户下运行，从而可使 VM 和主机操作系统彼此不受影响。通过 WSv，主机操作系统将得到保护，出现安全问题的 VM 对其他 VM 产生的损坏也会受到限制。

1.2.2 强大的隔离能力

服务器虚拟化使具有不同资源要求的工作负载能够在同一主机服务器上共存。WSv 提供了多种功能，便于高效地使用主机服务器的物理资源。

- 灵活的内存分配：可以为虚拟机分配 RAM 的最大值和必须保证的最小值。此功能允许管理员创建 WSv 配置来依据整体 WSv 服务器性能平衡单个 VM 资源需求。
- 动态的硬件添加：WSv 可以在受支持的来宾操作系统运行时向其动态添加逻辑处理器、内存、网络适配器和存储器。此功能便于对来宾操作系统精确分配 WSv 主机处理能力。
- 灵活的网络配置：WSv 为 VM 提供高级的网络功能，包括 NAT、防火墙和 VLAN 分配。这种灵活性可用于创建更好地支持网络安全要求的 WSv 配置。

WSv 灵活的内存分配、动态的硬件添加和灵活的网络配置功能便于更高效地响应动态服务器负载。例如，阶段结束时的处理工作负载通常比某些业务线(Line of Business，LOB)应用程序工作负载的平均值高好几倍。WSv 可与受支持的来宾操作系统一起使用为运行的 VM 动态分配附加内存和处理器资源，并且无须重新启动来宾操作系统即可处理扩展的处理要求。只要主机服务器资源充足，此更改不会降低主机上运行的其他 VM 的性能。

1.2.3 性能

与早期版本相比，设计的改进以及与支持虚拟化的硬件集成使 WSv 能够虚拟化那些具有更高要求的工作负载，并且在资源分配中具有更大的灵活性。

性能的改进包括以下内容。

- 基于 64 位管理程序的轻型、低开销虚拟化体系结构：支持虚拟化的硬件(Intel VT 和 AMD Pacifica 技术)实现了更高的来宾操作系统性能。
- 多核心支持。可以为每个 VM 分配多达 8 个逻辑处理器，这样，就可以利用多处理器 VM 核心的并行处理优势，对要求大量计算的大型工作负载进行虚拟化。
- 64 位主机和来宾操作系统支持：在 64 位版本的 Windows Server 2008 上运行时，WSv 可提供对来宾 VM 的大型内存池的访问。在 WSv 下，可以成功虚拟化在 32 位操作系统上执行时会出现大量分页的非常耗费内存的工作负载。WSv 还支持在同一合并服务器上同时运行 64 位和 32 位来宾

操作系统。

- 服务器核心(Server Core)支持。WSv 可以将 Windows Server 2008 的服务器核心安装成为主机操作系统。服务器核心具有最低安装需求和低开销，旨在提供尽可能多的主服务器处理能力来运行 VM。
- 传递磁盘访问。可以将来宾操作系统配置为直接访问本地或 iSCSI 存储区域网络(SAN)存储，为产生大量 I/O 操作的应用程序(如 SQLServer 或 Microsoft Exchange)提供更高的性能。

许多服务器工作负载对服务器处理和 I/O 子系统要求较高。过去，SQL Server 和 Microsoft Exchange 之类的工作负载通常需要较大的内存和磁盘吞吐量，因此虚拟化这些工作负载有一定难度。WSv 中的 64 位管理程序以及传递磁盘访问等功能通常适用于虚拟化大型工作负载。

1.2.4　简化的管理

在部署 WSv 的数据中心和远程分支机构安装中，需要强大的管理功能和自动化功能来完全实现虚拟化以降低成本。WSv 通过以下管理功能和自动化功能满足此需求。

- 可扩展管理：WSv 可以与 Microsoft System Center Operations Manager(SCOM)和 System Center Virtual Machine Manager(SCVMM)协同工作。这些管理工具为 WSv 提供报告、自动化、部署和用户自助式工具。
- 用于 VM 管理的 MMC 3.0：熟悉的 Microsoft 管理控制台(Microsoft Management Console，MMC)界面用于管理 WSv 配置和 VM 设置，这样可极大地缩短学习 WSv 的时间。
- Windows Management Instrumentation(WMI)界面：WSv 包含 WMI 提供程序，该提供程序提供系统信息和可脚本化的管理访问。
- PowerShell 脚本：WSv 主机和 VM 配置可以通过 Windows PowerShell 配置。
- 组策略对象(GPO)管理：WSv 使用 GPO 的配置管理功能管理 WSv 主机虚拟化和虚拟机配置。

通过 SCOM 和 SCVMM 的管理功能，可以有效地管理 WSv 的数据中心安装和高度分散的安装。例如，可以使用对 WSv 中 WMI 提供程序的脚本访问通过以下方式来自动维护多个 WSv 主机服务器上的窗口：关闭来宾 VM 并在备用服务器上启动它们、执行主机服务器维护，然后在原始主机上恢复这些虚拟机。由于添加了 System Center Virtual Machine Manager，此操作可以自动执行，不需要中断许多应用程序。

1.3　Web 和应用程序平台

Windows Server 2008 为开发和可靠地承载通过服务器或 Web 传送的应用程序和服务提供了一个安全、易于管理的平台。其新增功能包括：简化的管理、提高的安全性以及性能和可扩展性的改进。此外，企业还将享受到更有效的应用程序和服务管理、更快的 Web 应用程序和服务部署及配置，以及更安全、简化、自定义的 Web 平台。Windows Server 2008 为 Web 应用程序和服务提供了更高的性能和可伸缩性，同时允许管理员更好地控制和监视应用程序和服务利用关键操作系统资源的情况。

Internet Information Services 7.0(IIS 7.0 或 IIS7)新特性

图 1-3 展示了 IIS 7.0 的新特性。Windows Server 2008 为 Web 发布提供了统一的平台，此平台集成了

Internet Information Services 7.0(IIS 7.0 或 IIS7)、ASP.NET、Windows Communication Foundation 以及 Microsoft Windows SharePoint Services。对现有的提供 IIS 服务的 Web 服务器而言，IIS 7.0 是一个很大的进步，它在集成 Web 平台技术中担任核心角色。IIS 7.0 的主要优点是提供了更有效的管理功能、改进了安全性和降低了支持成本。这些功能有助于创建一个为 Web 解决方案提供单一、一致的开发和管理模型的统一平台。

1. 改进的管理工具

图 1-4 展示了 IIS 7.0 管理过程中的各个环节的改进，IIS 7.0 中新的管理实用工具 IIS 管理器是更有效的 Web 服务器管理工具。它提供了对 IIS 和 ASP.NET 配置设置、用户数据和运行时诊断信息的支持。新的用户界面还支持托管或管理网站的用户将管理控制权委派给开发人员或内容所有者，从而可减少拥有成本和管理员的管理负担。新的 IIS 管理器界面支持通过 HTTP 进行远程管理，从而允许进行集成的本地、远程甚至跨 Internet 的管理，而不要求在防火墙中打开 DCOM 或其他管理端口。



图 1-3　IIS 7.0 的新特性



图 1-4　IIS 7.0 管理中各个环节的改进

此外，还包含新增的命令行工具——appcmd.exe，它用于管理 Web 服务器、网站和 Web 应用程序。此命令行界面简化了管理员常见的 Web 服务器管理任务。例如，可以使用 appcmd.exe 列出已被迫等待 500 ms 以上的 Web 服务器请求。此信息可用于对性能欠佳的应用程序进行故障排除，可将 appcmd.exe 的输出通过管道传递给其他命令，以便进一步处理。

2. 基于模块功能的安装

IIS 7.0 由 40 多个单独的功能模块构成。其中仅一半左右的模块是默认安装的，管理员可以有选择地安装或删除任何选择的功能模块。此模块化方法允许管理员仅安装所需选项，并且通过限制需要管理和更新的功能数量来节省时间。此外，由于未运行不必要软件，减少了 Web 服务器的攻击面，提高了安全性。

3. 分布式配置模型

图 1-5 展示了可远程管理 IIS 7.0 的 Web 服务器场，IIS 7.0 在如何存储和访问其配置数据方面做出了重大改进。IIS 7.0 版本的主要目标之一就是实现 IIS 设置的分布式配置，允许管理员在存储代码和内容的文件中指定 IIS 配置设置。

通过分布式配置，管理员可在存储代码和内容的目录中为网站或应用程序指定配置设置。通过在一个文件中指定配置设置，分布式配置允许管理员将所选网站功能或 Web 应用程序的管理权委派给其他人。例如，可以委派网站以便应用程序开发人员配置此网站使用的默认文档。管理员还可锁定特定配置设置，以

防止其他人对其进行更改。此功能可用于确保防止脚本执行的安全策略不被委派了网站管理访问权限的内容开发人员重写。通过使用分布式配置，在从开发到测试然后到最终进行生产的过程中迁移应用程序时，可将特定网站或应用程序的配置设置从一台计算机复制到另一台计算机。



图 1-5　用 IIS 7.0 管理网络

4. 诊断和故障排除

通过内置的诊断和跟踪支持，IIS 7.0 在对 Web 服务器进行故障排除时比以前更轻松，管理员可以监视 Web 服务器并查看详细的实时诊断信息。在进行诊断和故障排除时，开发人员或管理员可查看在服务器上运行的请求。IIS 7.0 还包含新增的 RuntimeStatus(运行时状态)和 Control(控件)对象，它们提供有关应用程序池、工作进程、站点、应用程序域甚至运行的请求实时状态信息。例如，可以使用此信息确定工作进程中哪个请求占用了 CPU 资源的 100%。

IIS 7.0 还包含整个请求和响应路径中的详细跟踪事件，开发人员和管理员可以跟踪某个请求进入 IIS 请求处理管道、进入任何现有的页面级代码，然后返回响应的整个过程。通过这些详细的跟踪事件，开发人员不仅可以了解请求路径和伴随请求产生的错误信息，还可以了解已用时间和其他调试信息，以便对所有类型的错误进行故障排除。

IIS 7.0 还通过提供更详细和更具操作性的错误消息简化了故障排除。IIS 7.0 中的新自定义错误模块允许将详细错误信息发送回浏览器(默认情况下发送到本地主机)，还可以配置为发送到其他远程客户端。现在，管理员可以查看关于请求的详细信息、哪些潜在的问题可能导致此错误以及如何解决此错误的建议，而不只是查看简单的错误代码。

运行时状态和控件 API(RSCA)是帮助提高 IIS 7.0 故障排除支持的最重要功能之一，此功能提供来自 IIS 7.0 内部的有关服务器的详细运行信息。使用 RSCA，可以检查和管理各种实体，包括站点、应用程序池甚至.NET 应用程序域。RSCA 还实时显示当前正在服务器上执行的请求。RSCA 数据可从 WMI 提供程序和托管 API(Microsoft.Web.Administration)处获取。IIS 7.0 管理 GUI 和命令行工具也可为管理员提供此数据。

5. 可扩展的模块化体系结构

在早期版本的 IIS 中，所有功能默认情况下都是内置的，因此难以对任何此类功能进行扩展或替换。如前所述，在 IIS 7.0 中，核心分为 40 多个单独的功能模块。另外，核心还包括一个新的 Win32API，用于构建核心服务器模块。核心服务器模块是 Internet 服务器应用程序编程接口(ISAPI)过滤器和扩展的新的、

功能更强大的替代品。ISAPI 过滤器和扩展在 IIS 7.0 中仍受支持。由于所有 IIS 核心服务器功能都是使用新的 IIS 7.0Win32 模块 API 作为独立的功能模块开发的，因此用户可以添加、删除甚至替换 IIS 功能模块。

6. 用于自定义的灵活的可扩展模型

IIS 7.0 使开发人员能够扩展 IIS 以通过新的、更有力的方式提供自定义功能。这在一定程度上归功于全新的核心服务器应用程序编程接口(API)集，它允许功能模块既可以使用本机代码(C/C++)开发，也可以使用托管代码(如使用.NET Framework 的 C#和 Visual Basic 2005 等语言)开发。事实上，用于请求和应用程序处理的 IIS 7.0 功能集中的大部分功能就是使用这些相同的 API 实现的。IIS 7.0 还实现了配置、脚本、事件日志记录和管理工具功能集的可扩展性，从而为软件开发人员提供可在其上构建 Web 服务器扩展的、完善的服务器平台。

7. 真正的应用程序 xcopy 部署

IIS 7.0 允许将 IIS 配置设置存储在 web.config 文件中，这样更易于使用 xcopy 在多个 Web 服务器间复制应用程序，并可避免执行成本高且易于出错的复制、手动同步和其他配置任务。

8. 摘要

IIS 7.0 中的所有结构更改一起创建了一个极其灵活的 Web 应用程序系统，这为只具备基本技能的 Web 服务器管理员新手和使用脚本工具管理多个服务器的高级管理员，通过 GUI 界面和 appcmd.exe 命令行工具访问 IIS 配置的功能提供了有效的工具。IIS 的跟踪和故障排除组件提供了详细的可用信息，可帮助管理员和应用程序开发人员隔离行为错误的页和代码。IIS 7.0 的模块化功能和详细的管理模型便于服务器管理员创建满足自己需要的服务器，并只允许对站点和内容管理器进行所需级别的访问。

1.4　服务器管理

从简化新服务器的配置到自动执行重复的管理任务，简化复杂的日常服务器管理是 Windows Server 2008 中包括的许多增强功能的关键主题。集中式管理工具、直观的界面和自动化功能使 IT 专业人员能够在中央网络和远程位置(如分支机构)更轻松地管理网络服务器、服务和打印机。

1. 初始配置任务

使用 Windows Server 2008，简化的安装过程不会被需要用户干预的配置任务中断。现在，那些任务和对话框在完成基本安装后出现，这样管理员也不必就安装顺序进行交互。

“初始配置任务”(Initial Configuration Tasks)窗口是 Windows Server 2008 的新功能，可以帮助管理员预先配置和设置新服务器。它包括一系列任务，例如设置管理员密码、更改管理员账户的名称以提高服务器的安全性，将服务器加入现有域以及启用 Windows Update 和 Windows 防火墙。

2. 服务器管理器控制台

通过新的服务器管理器控制台，Windows Server 2008 简化了在组织中管理和保护多个服务器角色的任务。服务器管理器控制台提供一个统一的控制台，用于管理服务器的配置和系统信息、显示服务器状态、确定服务器角色配置的问题以及管理在服务器上安装的所有角色。

服务器管理器控制台的层次结构窗格包含可扩展节点，管理员可以使用这些节点直接进入控制台来管

理特定角色、对工具进行故障排除或查找备份和灾难恢复选项。

服务器管理器将各种管理界面和工具合并到统一的管理控制台中，使管理员不必在多个界面、工具和对话框之间导航即可完成常见管理任务。

3. 服务器管理器向导

与 Windows Server 早期版本相比，服务器管理器中的向导通过缩短部署时间简化了企业中的服务器部署任务。现在，大部分常见配置任务(如配置或删除角色、定义多个角色和角色服务)可以使用服务器管理器向导在单个会话中完成。

Windows Server 2008 在用户使用服务器管理器向导的过程中会执行相关性检查，确保安装了所选角色需要的所有必备角色服务，并且未删除任何可能仍然需要的剩余角色或角色服务。

4. Windows PowerShell

Microsoft Windows PowerShell 命令行外壳和脚本语言可帮助 IT 专业人员自动执行常见任务，如图 1-6 所示。通过使用新的侧重管理的脚本语言、120 多种标准命令行工具以及一致的语法和实用工具，Windows PowerShell 使 IT 专业人员可以更轻松地控制系统管理和加速自动化。Windows PowerShell 易于采用，因为它利用现有 IT 基础结构和现有脚本投资。它允许用户自动执行基本服务器管理任务以及特定服务器角色(如终端服务器)的系统管理。

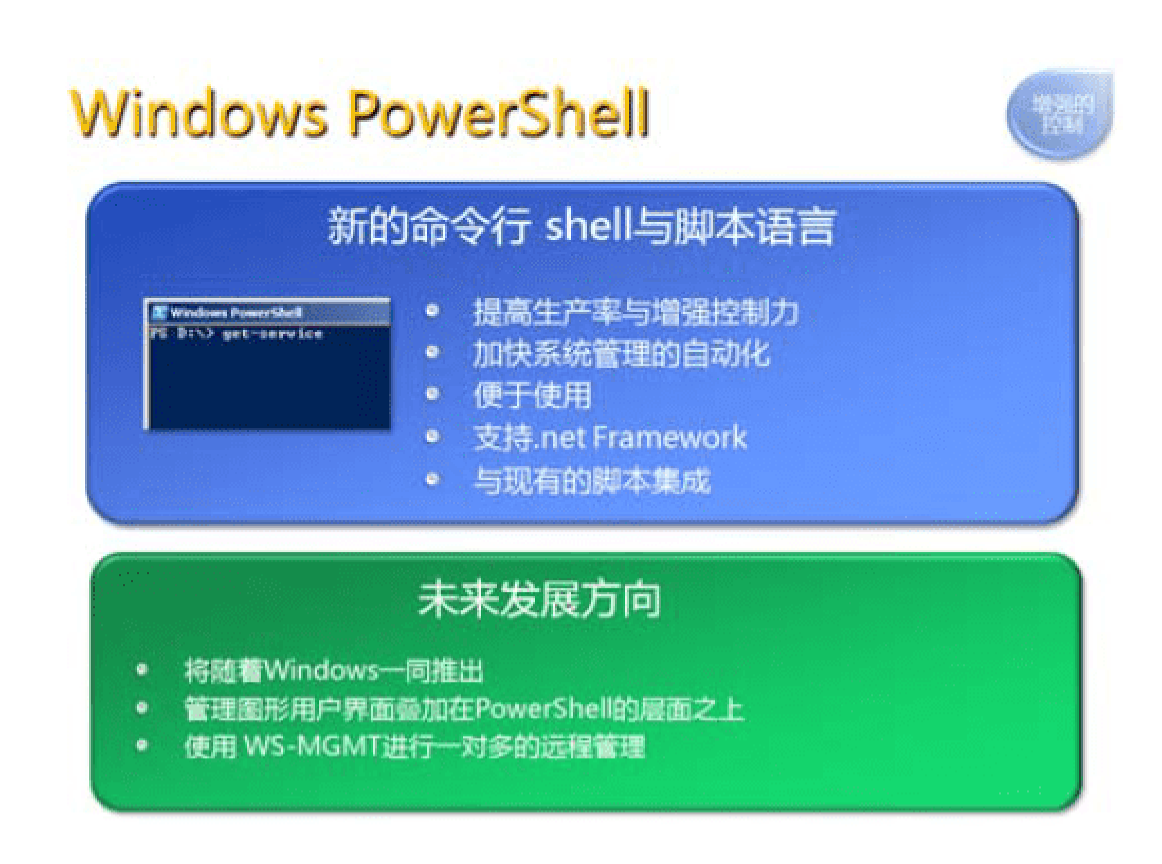


图 1-6　Windows PowerShell 简介

Windows PowerShell 集成了命令行外壳和脚本语言，这使管理员可以更高效地完成和自动执行批量系统管理任务。Windows PowerShell 通过提供与脚本语言具有完全相同的语法的 cmdlet(命令行工具)对 Windows 命令提示和 Windows ScriptHost(WSH)进行了改进。在 Windows PowerShell 命令行中输入的命令与为了在多个服务器上自动执行任务而在脚本中使用的命令相同。

PowerShell 支持组织的现有脚本(例如，.vbs、.bat、.perl)，因此组织不需要迁移脚本即可采用 PowerShell。现有的基于 Windows 的命令行工具将从 PowerShell 命令行运行。通过提供一致的语法和命名约定以及脚本语言与交互式外壳的集成，PowerShell 降低了自动执行系统管理任务的复杂度，缩短了执行这些任务所需的时间。

5. Windows 远程管理(WS-Management)

随着分支机构和其他位置中的远程服务器数量的增加，IT 专业人员需要更好的方法来高效地管理非现

场服务器。Windows 远程管理提供了一种低带宽、可脚本化的方法来轻松管理远程位置的服务器。

Windows Remote Manager 是 Microsoft 在 WS-Management 协议(允许硬件和操作系统进行交互操作的基于 SOAP 的标准协议)的基础上实现的。管理员可以使用 Windows 远程管理脚本对象、Windows 远程管理命令行工具或 Windows RemoteShell 命令行工具从本地和远程计算机中获取管理数据(例如，有关磁盘、网络适配器、服务或进程等对象的信息)。如果计算机运行的是包括 Windows 远程管理的 Windows 操作系统版本，则管理数据由 Windows Management Instrumentation(WMI)提供。

1.5 服务器核心

从 Windows Server 2008 开始，管理员可以选择安装具有特定功能但不包含任何不必要功能的 Windows Server 的最小安装。服务器核心(Server Core)提供了运行以下一个或多个服务器角色的环境。

- Windows Server 虚拟化。
- 动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)服务器。
- 域名系统(Domain Name System，DNS)服务器。
- 文件服务器。
- Active Directory 目录服务(Active Directory Directory Service，ADDS)。
- Active Directory 轻型目录服务(Active Directory Light Directory Service，ADLDS)。
- Windows 媒体服务。
- 打印管理。

Server Core 可为组织提供以下好处。

- 减少了软件维护。因为服务器核心仅安装使可管理的服务器运行支持的服务器角色所需的功能，所以服务器需要较少的软件维护。由于使用的是较小的服务器核心安装，更新和修补程序的数量也相应减少，这样既节省了服务器使用的 WAN 带宽又缩短了 IT 人员的管理时间。
- 减小了攻击面。因为减少了在服务器上安装和运行的文件，所以暴露给网络的攻击目标也有所减少；因此，攻击面也相应减小。管理员可以只安装给定服务器所需的特定服务，将暴露风险降低到最低值。
- 减少了要求重新启动的次数，减小了所需的磁盘空间。使用最小的服务器核心安装时，需要更新或修补的已安装组件有所减少，需要重新启动的次数也相应减少。服务器核心安装只安装提供所需功能需要的最少文件，所以减小了在服务器上使用的磁盘空间。通过选择在服务器上使用服务器核心安装选项，管理员可以降低服务器的管理和软件更新要求，同时降低安全风险。
- 使用 Windows Server 2008 中的服务器核心安装选项，管理员可以降低服务器的持续维护要求并简化其管理。通过运行仅限于所需功能的最小服务器核心安装，IT 人员只需为该服务器安装直接影响安装文件的修补程序和更新。

1.6 Windows Server 2008 打印管理

组织越大，网络内的打印机数量越多，IT 人员安装和管理那些打印机需要花费的时间也就越多；所有这些都会增加运营支出。Windows Server 2008 包括打印管理，它是一个 MMC 管理单元，使管理员能够

通过一个界面来管理、监视组织内的所有打印机(甚至远程位置的打印机)以及对其进行故障排除。

打印管理在一个控制台中提供有关网络上所有打印机和打印服务器状态的最新详细信息。打印管理可以帮助查找出现错误状况的打印机，还可以在打印机或打印服务器需要引起关注时发送电子邮件通知或运行脚本。在提供 Web 界面的打印机模型上，打印管理可以访问此附加数据。这样就可以轻松地管理信息(如墨粉和纸张量)，即使打印机位于远程位置。此外，打印管理可以在本地打印服务器的本地子网上自动搜索和安装网络打印机。

在客户端计算机上安装打印机以及管理和监视打印机时，打印管理可以为打印管理员节省大量时间。打印管理可与组策略结合使用来自动将打印机连接添加到客户端计算机的“打印机和传真”文件夹，而不必在单独的计算机上安装和配置打印机连接。对于需要访问同一台打印机的大量用户(如同一部门中的用户或一个分支机构中的所有用户)而言，这是一种添加打印机的既高效又省时的方法。

打印管理中提供的用于安装、共享和管理打印机的自动选项和集中的控制界面简化了管理，减少了 IT 人员部署打印机所需的时间。

1.7 安全和策略实施

Windows Server 2008 具有许多用于改进安全性和符合性的功能。部分主要增强功能包括以下内容。

- 强制实现客户端正常运行。网络访问保护(Network Access Protection，NAP)使管理员可以在允许客户端访问网络之前配置和强制实现正常运行与安全要求。
- 监视证书颁发机构。企业 PKI 改进了监视多个证书颁发机构(Certificate Authority，CA)以及对其进行故障排除的功能。
- 防火墙增强功能。新的具有高级安全性的 Windows 防火墙提供了许多安全增强功能。
- 加密和保护数据。BitLocker 通过对磁盘驱动器加密来保护敏感数据。
- 加密工具。下一代加密技术提供了灵活的加密开发平台。
- 服务器和域隔离。服务器和域资源可以隔离，以限制对通过身份验证和授权的计算机进行访问。
- 只读域控制器(Read-Only Domain Control，RODC)。RODC 是新类型的域控制器安装选项，可以安装在具有较低级别的物理安全性的远程站点中。

这些改进可帮助管理员提高组织的安全级别，简化与安全相关的配置和设置的管理与部署。

1.7.1 网络访问保护

网络访问保护(Network Access Protection，NAP)可以防止不能正常运行的计算机访问组织网络和影响其安全性(参见图 1-7)。NAP 用于配置和强制实现客户端正常运行要求，以及在不符合要求的计算机连接到公司网络之前对其进行更新或修补。通过 NAP，管理员可以配置正常运行策略，这些策略定义连接到组织网络的计算机的软件要求、安全更新要求和所需的配置设置等内容。

NAP 通过评估客户端计算机的运行状况以及限制不符合要求的客户端计算机的网络访问来强制实现客户端正常运行要求。客户端和服务器端组件都可帮助对不符合要求的客户端计算机进行修补，以便获取不受限制的网络访问权限。如果确定某台客户端计算机不符合要求，则可以拒绝它对网络进行访问，或者立即对其进行修补以使其符合要求。

NAP 强制实现方法支持四种网络访问技术，它们与 NAP 结合使用来强制实现正常运行策略：Internet 协议安全(IPSec)强制、802.1X 强制、用于路由和远程访问的虚拟专用网络(Virtual Private Network，VPN)强制以及动态主机配置协议(DHCP)强制。

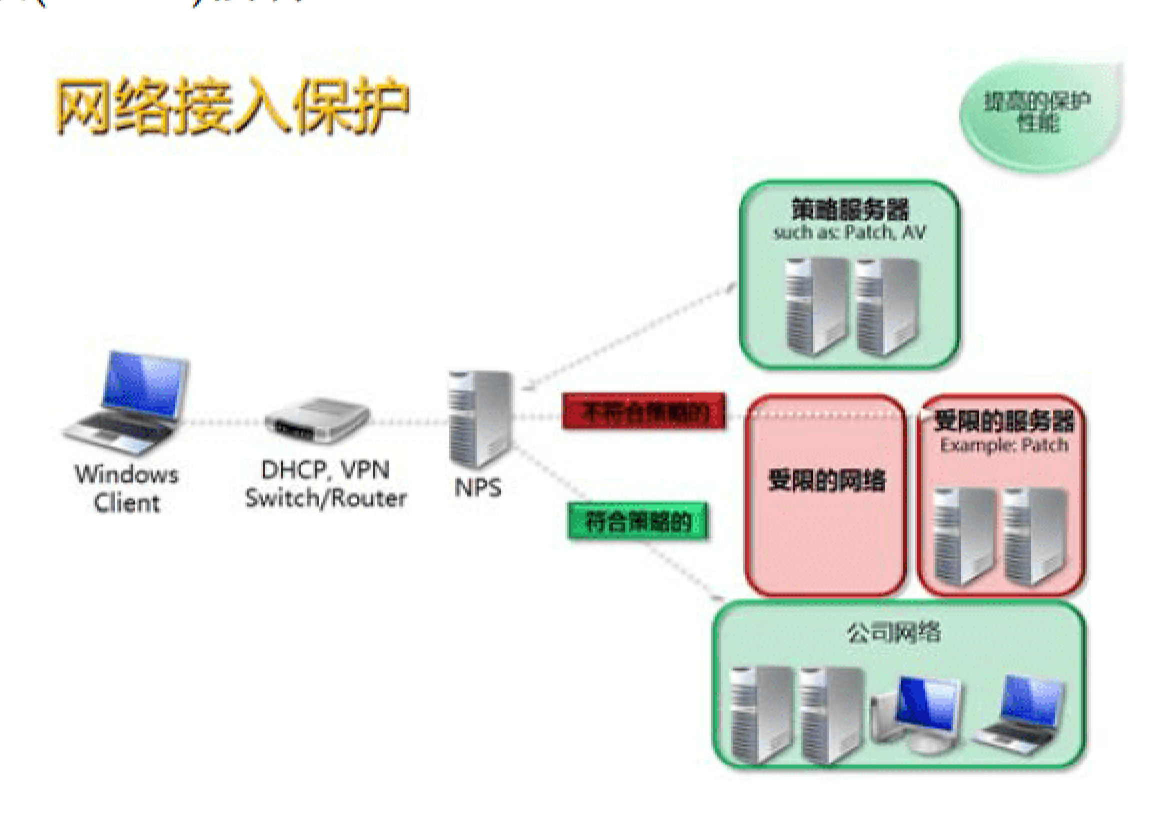


图 1-7　网络接入保护示意

1.7.2　Windows 防火墙高级安全功能

Windows Server 2008 中具有高级安全性的 Windows 防火墙是基于主机的状态防火墙，它依据其配置和当前运行的应用程序来允许或阻止网络通信，从而保护网络免遭恶意用户和程序的入侵。其新增功能如图 1-8 所示。



图 1-8　Windows 高级防火墙新增功能

其中一项新功能是支持防火墙对传入和传出通信进行拦截。例如，网络管理员可以对新的 Windows 防火墙配置一组例外情况，阻止所有通信发送到特定端口(如已知的由病毒软件使用的端口)或者发送到包含敏感内容或不希望被访问的内容的地址。这样可以使计算机免遭可能通过网络传播的病毒的入侵，并使网络免遭可能试图从出现安全问题的系统传播的病毒的入侵。

由于增加了大量 Windows 防火墙配置选项，因此增添了名为“具有高级安全性的 Windows 防火墙”的新 MMC 管理单元以简化管理。通过这一新的管理单元，网络管理员可以在客户端工作站和服务器上远程配置 Windows 防火墙设置(这在不具有远程桌面连接的早期版本中是无法实现的)，从而简化了远程配置

和管理。

在 Windows Server 早期版本中，Windows 防火墙和 IPSec 是分别配置的。由于基于主机的防火墙和 Windows 中的 IPSec 都能够阻止或允许传入通信，因此创建的防火墙例外和 IPSec 规则可能会重叠或矛盾。Windows Server 2008 中新的 Windows 防火墙使用相同的 GUI 和命令行命令合并了这两种网络服务的配置。防火墙和 IPSec 设置的这种集成简化了防火墙和 IPSec 配置，可防止出现策略重叠和矛盾设置。

1.7.3　BitLocker 驱动器加密

BitLocker 驱动器加密是 Windows Server 2008 中一个重要的新功能，可帮助保护服务器、工作站和移动计算机，如图 1-9 所示。Windows Vista Enterprise 和 Windows Vista Ultimate 版本中也提供了 BitLocker，用于保护客户端计算机和移动计算机。BitLocker 可对磁盘驱动器的内容加密。这样可以防止未经授权的使用者通过运行并行操作系统或运行其他软件工具绕过文件和系统保护，或者对存储在受保护驱动器上的文件进行脱机查看。



图 1-9　BitLocker 的作用

BitLocker 通过将两个主要子功能相结合增强了数据保护：系统卷加密和对早期引导组件的完整性检查。它对整个系统卷加密，包括交换和休眠文件，从而可提高分支机构中远程服务器的安全性。BitLocker 解决了从丢失、被盗或不适当地淘汰的 PC 中窃取或泄露数据的威胁。BitLocker 还有助于组织遵守政府法规(如 Sarbanes-Oxley 和 HIPAA)，这些法规要求对安全和数据保护进行极高标准的维护。

1.7.4　企业 PKI

Windows Server 2008 和 Windows Vista 操作系统提供了大量公钥基础结构增强功能。Windows PKI 的所有方面的可管理性都有所增强，吊销服务已经过重新设计，并且对注册的攻击面也有所降低，如图 1-10 所示。

PKI 的增强功能包括以下几项。

- 企业 PKI(PKIView)：最初是 Microsoft Windows Server 2003 ResourceKit 的一部分(曾称为 PKIHealth 工具)，现在，PKIView 是 Windows Server 2008 的一个 Microsoft 管理控制台(MMC)管理单元。它用于分析 CA 的运行状态，并可查看在 ADCS 中发布的 CA 证书的详细信息。
- 联机证书状态协议(Online Certificate Status Protocol，OCSP)：基于联机证书状态协议(OCSP)的联机响应程序可用于管理和分发传统 CRL 不是最佳解决方案时的吊销状态信息。联机响应程序

可以在单台计算机上或联机响应程序组中进行配置。

- 网络设备注册服务(Network Device Enrollment Service，NDES)：在 Windows Server 2008 中，网络设备注册服务(NDES)是 Microsoft 基于简单证书注册协议(Simple Certificate Enrollment Protocol，SCEP)实现的。该协议是一种使软件可以在网络设备(如路由器和交换机)上运行的通信协议，如果没有该协议，在网络上将不能通过身份验证来注册证书颁发机构(CA)颁发的 x509 证书。
- Web 注册：与早期版本相比，新的 Web 注册控制更安全、更易于编写脚本并且更易于更新。
- 组策略和 PKI：组策略中的证书设置使管理员能够从域中所有计算机的一个中央位置来管理证书设置。

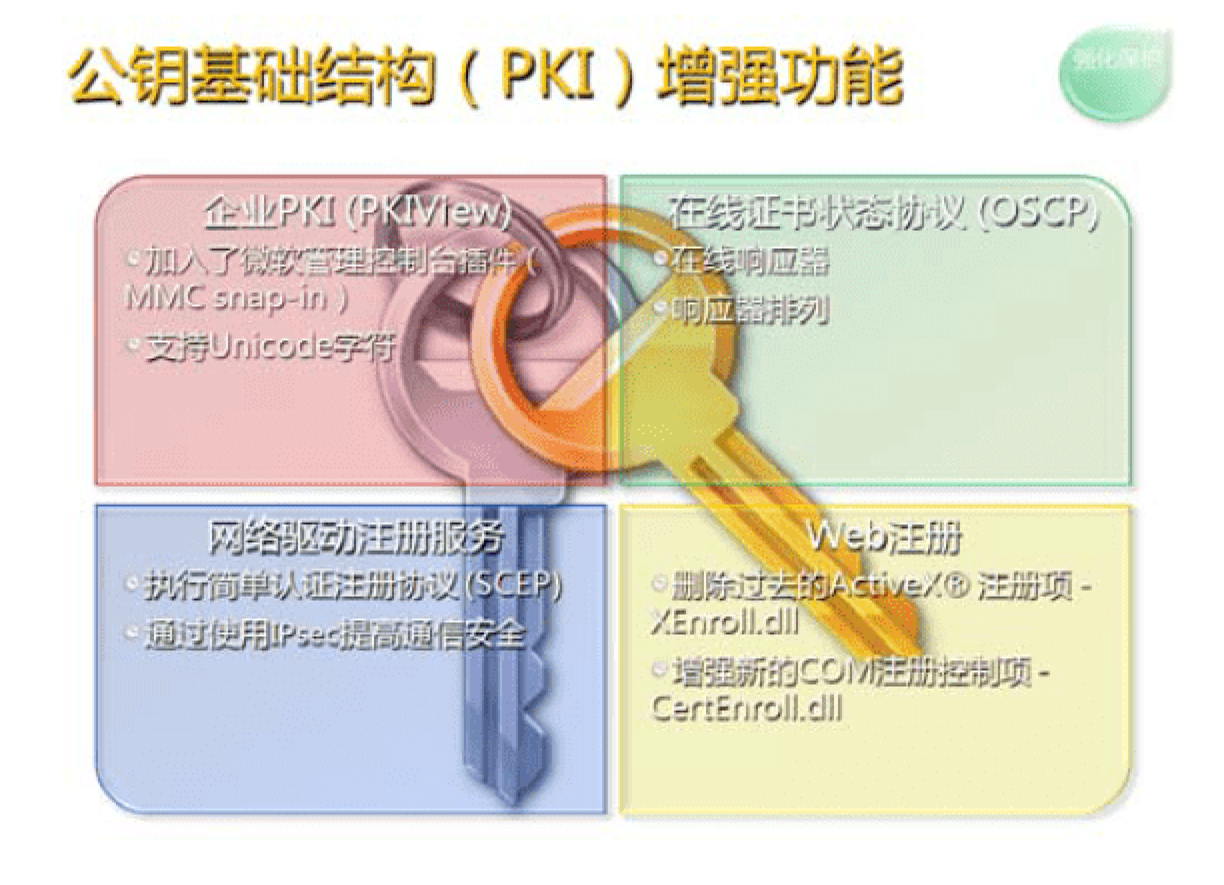


图 1-10　公钥基础结构(PKI)增强功能

1.7.5　下一代加密技术

如图 1-11 所示，下一代加密技术(Cryptography Next Generation，CNG)提供了灵活的加密开发平台，允许 IT 专业人员在与加密相关的应用程序(如 Active Directory 证书服务(Active Directory Certificate Service，ADCS)、安全套接字层(Secure Socket Layer，SSL)和 Internet 协议安全(Internet Protocol Security，IPSec))中创建、更新和使用自定义加密算法。CNG 实施美国政府的 SuiteB 加密算法，其中包括加密算法、数字签名算法、密钥交换算法和哈希算法。

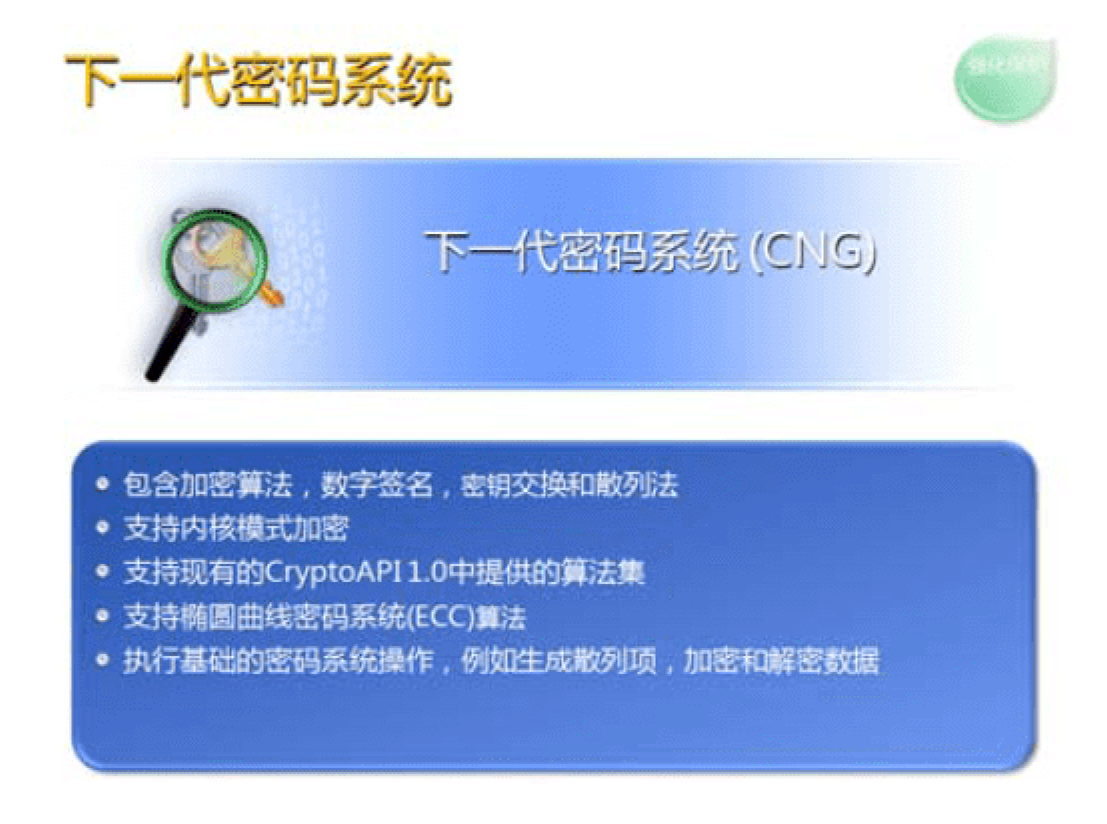


图 1-11　下一代密码系统

CNG 提供了一组 API，可用于执行基本加密操作，如创建、存储和检索加密密钥。它还支持其他加密提供程序的安装和使用。CNG 使组织和开发人员既能够使用自己的加密算法，也能够实现标准加密算法。

CNG 支持现在的 CryptoAPI 1.0 算法集，还支持椭圆曲线加密(Elliptic Curves Cryptography，ECC)算法。美国政府的 SuiteB 成果需要使用大量的 ECC 算法。

1.7.6　只读域控制器

只读域控制器(RODC)是 Windows Server 2008 操作系统中提供的一种新类型的域控制器，主要用于在分支环境中进行部署。如图 1-12 所示，通过 RODC，组织可以降低在无法保证物理安全的远程位置(如分支机构)中部署域控制器的风险。



图 1-12　只读域控制器

除账户密码外，RODC 可以驻留可写域控制器驻留的所有 Microsoft Active Directory 域服务(ADDS)对象和属性。不过，客户端无法将更改直接写入 RODC。由于更改不能直接写入 RODC，因此不会发生本地更改，作为复制伙伴的可写域控制器不必从 RODC 导入更改。管理员角色分离指定可将任何域用户委派为 RODC 的本地管理员，而无须授予该用户对域本身或其他域控制器的任何用户权限。

1.7.7　服务器和域隔离

在基于 Windows 的网络中，管理员可以在逻辑上隔离服务器资源和域资源，以限制对通过身份验证和授权的计算机的访问。例如，可在现有的物理网络中创建一个逻辑网络，其中计算机共享一组相同的要求以便安全地通信。在这个逻辑上隔离的网络中，每台计算机必须向该隔离网络中的其他计算机提供身份验证凭据以便建立连接。

这种隔离可防止未授权计算机和程序不恰当地获取资源的访问权限。来自不属于隔离网络的计算机的请求将被忽略。服务器和域隔离可帮助保护特定的高价值服务器和数据，也可使托管计算机免遭未托管或恶意的计算机和用户破坏。

可使用以下两种类型的隔离来保护网络。

- 服务器隔离：在服务器隔离方案中，使用 IPSec 策略将特定服务器配置为仅接受来自其他计算机的通过身份验证的通信。例如，可将数据库服务器配置为仅接受来自 Web 应用程序服务器的连接。
- 域隔离：要隔离域，管理员可以使用 Active Directory 域成员身份，确保作为域成员的计算机仅接受来自作为域成员的其他计算机的通过身份验证的安全通信。隔离网络仅由属于该域的计算机组成。域隔离使用 IPSec 策略为域成员(包括所有客户端计算机和服务器计算机)之间发送的通信提供保护。

通过 Windows Server 2008，组织可以使用基于安全功能(如网络访问保护)的策略获得前所未有的安全性。评估和控制连接计算机的运行状况和安全状态将为组织提供重要的安全改进。Windows Server 2008 中新的管理界面简化了配置和维护组织内多台服务器的管理过程，从而可降低管理企业网络安全所需的成本。

1.8 集中式应用程序访问

Windows Server 2008 对终端服务(Terminal Services，TS)进行了改进和创新，它不再仅仅能够访问应用程序，而且允许用户在自己的桌面上并行运行远程应用程序和本地应用程序，从而可改善用户体验。它还提供了用于通过 Terminal Services Web Access 集中访问可用的应用程序的新选项。

新的终端服务组件包括以下几项。

- Terminal Services RemoteApp：通过使用新的 Remote Desktop Connection 6.0(远程桌面连接 6.0 版)客户端，Terminal Services RemoteApp 允许用户在其桌面上并行运行本地应用程序和远程访问的 Windows 程序。
- 终端服务网关：无须虚拟专用网络(VPN)基础结构，终端服务网关(TS 网关)即可提供对终端服务器和共享桌面的安全访问，从而将终端服务的范围扩展到了公司防火墙以外。
- Terminal Services WebAccess：Terminal Services Web Access(TS Web Access)提供了一个远程应用程序解决方案，此方案简化了管理员发布远程应用程序的过程，同时还简化了用户查找和运行远程应用程序的过程。
- 单一登录：使用单一登录，不必再重复输入凭据，从而可改善远程用户的用户体验。

1.8.1 终端服务

Windows Server 2008 终端服务包含新增的核心功能，改善了最终用户连接到 Windows Server 2008 终端服务器时的体验。新增的核心功能包括以下几项。

- Remote Desktop Connection 6.0：要访问终端服务，用户需要使用 Remote Desktop Connection 6.0。它随 Windows Server 2008 和 Windows Vista 一起提供，Windows XP 用户和 Windows Server 2003 用户可免费下载。
- 远程桌面连接显示改进：Remote Desktop Connection 6.0 软件支持使用较高分辨率(最高到 4096×2048)的桌面计算机，还支持水平跨越多个监视器组成一个大桌面。Remote Desktop Connection 6.0 用户可使用较新的高分辨率监视器和与以前的 4∶3 标准不符的新潮显示格式(如 16∶9 或 16∶10 宽屏幕格式)。
- 桌面体验：Remote Desktop Connection 6.0 可在用户的客户端计算机上重现远程计算机的桌面。

在 Windows Server 2008 中安装"桌面体验"(Desktop Experience)后，用户可在其远程连接中使用 Windows Media Player、桌面主题和照片管理等 Windows Vista 功能。"桌面体验"功能和数据优先级显示设置(用于保持键盘、鼠标与监视器上显示的内容同步，即使在带宽使用率非常高的情况下也是如此)增强了最终用户连接到 Windows Server 2008 终端服务器时的体验。

1. 单一登录

使用单一登录，具有域账户的用户除第一次登录到终端服务会话时要使用密码或智能卡外，以后再访问远程服务器和应用程序时，系统不会提示其输入凭据。单一登录无须用户每次启动远程会话时都输入凭据，从而可改善用户体验。

2. Terminal Services RemoteApp

Terminal Services RemoteApp 是 Windows Server 2008 提供的一种新的远程应用程序显示方法。RemoteApp 是终端服务显示方法的补充，它在窗口中向访问应用程序的用户显示整个远程桌面，如图 1-13 所示。



图 1-13　终端服务新增的 RemoteApp 服务

现在，远程应用程序(而非整个远程桌面)在客户端计算机桌面上该应用程序本身的可调整大小的窗口中启动和运行。如果程序使用了通知区域图标，图标会显示在客户端的通知区域中。弹出窗口被重定向到本地桌面，本地驱动器和打印机也被重定向并在远程程序中可用。许多用户可能不知道远程程序和在其桌面上与远程程序并行运行的其他本地应用程序有什么区别。

RemoteApp 仅维护服务器上的一个中心应用程序，而不需维护整个组织中多个桌面上的单个安装，因而减少了管理工作量。由于使得远程应用程序和客户端计算机桌面更顺利地集成，RemoteApp 还改善了用户体验。

3. 终端服务网关

终端服务网关(TS 网关)是一个终端服务角色，如图 1-14 所示，允许经授权的远程用户通过 Internet 连接到企业网络中的终端服务器和工作站。这样，组织可轻松又安全地使远程用户或外出工作的人员无须使用 VPN 连接就能访问所选的服务器和工作站。

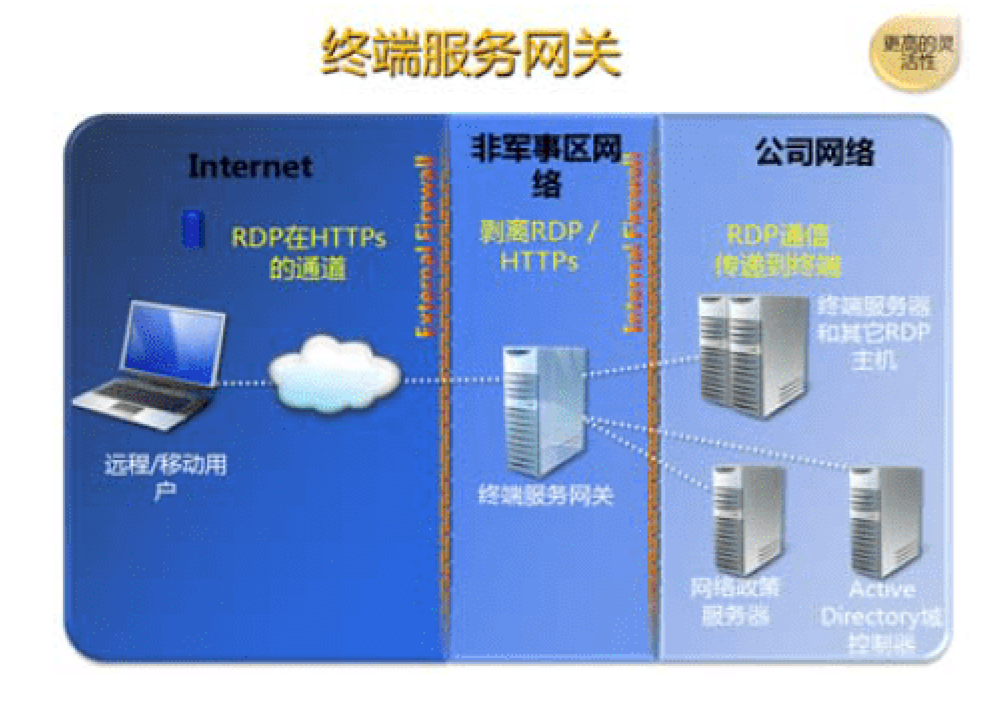


图 1-14 终端服务网关

TS 网关的一些主要技术特点如下。

- 使远程用户能通过 Internet 安全连接到企业网络资源，而无须复杂的虚拟专用网络(VPN)连接。
- 利用 HTTPS 协议的安全性和可用性提供终端服务，而无须进行客户端配置。
- 提供了一个全面的安全配置模型，管理员可使用此模型控制对网络中特定资源的访问。
- 使用户可穿过防火墙和网络地址转换器(Network Address Translation，NAT)远程连接到终端服务器和远程工作站。
- 提供了一个更加安全的模型，此模型允许用户仅访问所选的服务器和工作站，而不是通过 VPN 访问整个企业网络。

终端服务网关为组织提供了一种安全、轻松的方法，使远程用户无须安装和配置 VPN 连接即可访问网络中的服务器和工作站。使用全面的安全功能，管理员还可以控制对特定资源的访问。

1.8.2 Terminal Services Web Access

Terminal Services Web Access(TS Web Access)是一个终端服务角色，通过它，管理员可使用户无须安装任何软件就能通过 Web 浏览器访问 Terminal Services RemoteApp 程序。如图 1-15 所示，使用 TS Web Access，用户可访问网站以及所有可用应用程序列表。当用户启动列出的任一程序时，承载该应用程序的基于 Windows Server 2008 的终端服务器上会自动为用户启动一个终端服务会话。对用户而言，此 Web 界面提供了一个显示所有当前可用远程应用程序的集中式菜单，而且运行远程应用程序与在菜单中选择程序一样简单。

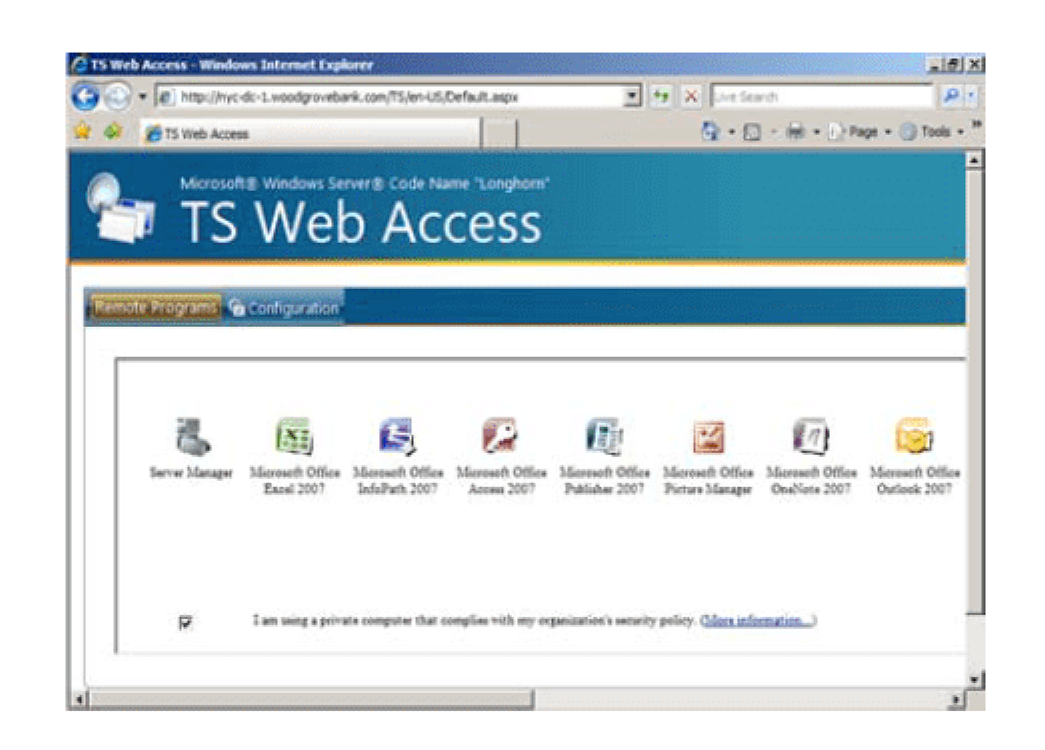


图 1-15 终端服务 Web 访问

使用 TS Web Access 可减少管理开销，还可从中心位置轻松访问程序。由于程序是在终端服务器而非在客户端计算机中运行，所以 IT 人员只需维护和更新该应用程序的一部分。

1.9　分支机构

企业希望更加贴近客户，因而正逐渐将工作人员从中心位置分散到各分支机构。如图 1-16 所示，随着分支机构数量不断增加，对这些远程位置的 IT 管理需要和安全关注也相应增长。Microsoft 意识到了这种快速增长的生产力因素，以及为应对特定的分支机构挑战所需新的解决方案的需要。



图 1-16　Windows Server 2008 对分公司的支持

由于分支机构现场的 IT 工作人员数量很少或根本就没有，因此，对这些分支机构中的服务器，IT 管理员需要考虑若干方面的问题。服务器上运行的软件必须有效地使用较低速的 WAN(Wide Area Network，广域网)连接，而不能占用所有带宽、延缓关键任务数据传输或对分支用户的应用程序体验产生负面影响。由于不能总是保证服务器的物理安全，所以，在分支机构中，安全性是一个要考虑的大问题。由于现场没有较多的 IT 工作人员，因而能提供集中管理及远程管理和部署的服务器解决方案比较适合分支机构。

在 Windows Server 2003 R2 中，Microsoft 开始解决分支机构方案的需求和挑战。Windows Server 2008 版本包括许多附加的改进，这些改进使管理员对分支机构的控制能力更强，并提高了对分支机构和组织的中心网络和数据的保护级别。它还为需要满足其组织独特需求的 IT 专业人士提供了更大的灵活性。

对于分支机构，Windows Server 2008 提供的主要好处可分为以下三个类别。

- 提高分支机构服务器部署和管理的效率。
- 降低分支机构中的安全风险。
- 提高 WAN 通信的效率和带宽使用率。

通过提供对关键服务器角色的简化部署和有效管理、改进的安全性以及一个可优化性能并可用于服务连续性的体系结构，Microsoft 的分支机构解决方案和 Windows Server 2008 的多种新功能和增强功能解决了基本的分支机构需求。

1.9.1　部署和管理

从远程位置管理服务器，服务和安全性是 IT 专业人士一直面临的挑战。Windows Server 2008 简化了

对位于分支机构中服务器的远程部署和持续管理。

Active Directory 目录服务的更改和增强功能、只读域控制器简介、BitLocker、角色分离和服务器核心安装选项是 Windows Server 2008 的特定功能，解决了分支机构的独特需求，并增加了 IT 部门远程管理的有效性。

1.9.2 只读域控制器

只读域控制器(Read-Only Domain Control，RODC)是 Windows Server 2008 操作系统提供的一种新类型的域控制器。RODC 主要是为在分支机构环境中部署而设计的。通过 RODC，组织可以限制在某些位置(例如，无法保证物理安全的分支机构)部署域控制器的风险。

除账户密码外，RODC 包含可写域控制器包含的所有 Microsoft Active Directory 域服务(ADDS)对象和属性。不过，客户端无法将更改直接写入 RODC。由于更改不能直接写入 RODC，因此不会发生本地更改，作为复制伙伴的可写域控制器不必从 RODC 导入更改。这样便减少了集线器网站中桥头服务器的工作负载以及监视复制所需的工作量。

管理员角色分离指定可委派任何域用户为本地 RODC 的管理员，而无须授予该用户任何对域本身或其他域控制器的用户权限。这样，便创建了以下方案：本地分支用户可在服务器上登录到 RODC 执行维护工作(如升级驱动程序)，而不必具有访问分支之外的域资源的权限。

1.9.3 BitLocker 驱动器加密

BitLocker 驱动器加密是 Windows Server 2008 中一项重要的新安全功能，可帮助保护分支机构中的服务器。Windows Vista Enterprise 和 Windows Vista Ultimate 版本中也提供了该功能，用于保护客户端计算机和漫游用户的移动计算机。BitLocker 可对磁盘驱动器的内容加密。这样可以防止未经授权的使用者通过运行并行操作系统或运行其他软件工具绕过文件和系统保护，或者对存储在受保护的驱动器上的文件进行脱机查看。

BitLocker 通过将两个主要子功能相结合增强了数据保护：系统卷加密和对早期引导组件的完整性检查。它对整个系统卷加密，包括交换和休眠文件，这样，增强分支机构中远程服务器的安全性。BitLocker 解决了从丢失、被盗或不适当地淘汰的 PC 中窃取或泄露数据的威胁。在分支机构方案中，这一点非常重要，因为不能总是保证服务器的物理安全。

1.9.4 服务器核心

从 Windows Server 2008 开始，管理员可以选择安装具有特定功能但不包含任何不必要功能的 Windows Server 的最小安装。

如图 1-17 所示的 Windows 服务器核心(Server Core)提供了运行以下一个或多个服务器角色(已全部在分支机构中部署)的环境。

- 动态主机配置协议(DHCP)服务器。
- 域名系统(DNS)服务器。
- 文件服务器。

- Active Directory 域服务(ADDS)。
- Active Directory 轻型目录服务(ADLDS)。
- Windows 媒体服务。
- 打印管理。
- Windows Server 虚拟化。

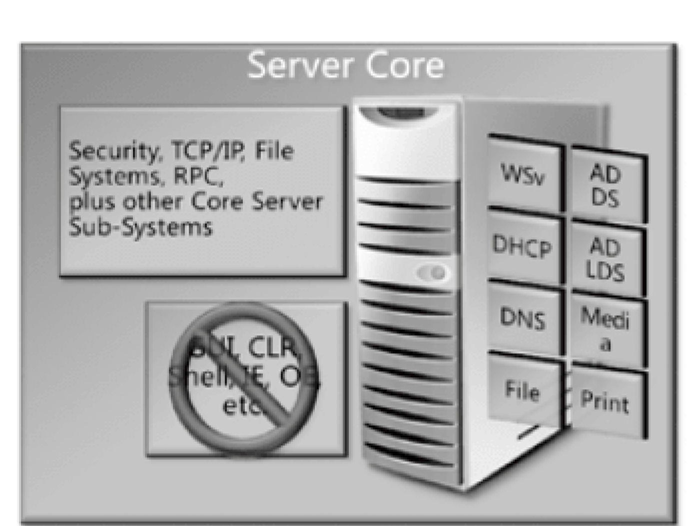


图 1-17 Windows Server Core 介绍

在分支机构方案中，使用服务器核心有以下好处。

- 减少了软件维护：执行较小的服务器核心安装减少了更新和修补程序的数量，从而可节省分支服务器占用的 WAN 带宽和 IT 工作人员耗费的管理时间。
- 减小了攻击面：管理员可以只安装其分支机构设置所需的特定服务，使暴露风险降至最小。
- 减少了要求重新启动的次数，减小了所需的磁盘空间：使用最小的服务器核心安装时，需要更新或修补的已安装组件有所减少，需要重新启动的次数也相应减少。服务器核心安装只安装提供所需功能需要的最少文件，所以将使用分支机构服务器上较少的磁盘空间。

1.9.5 增强 ActiveDirectory 的可管理性

Windows Server 2008 包括 ActiveDirectory 域服务中的改进，这些改进简化了域服务的管理，并为管理员解决分支机构的需求提供了更大的灵活性。一些关键的管理增强功能如下。

- 更新的 ActiveDirectory 域服务(ADDS)安装向导。
- 对用于管理 ADDS 的 Microsoft 管理控制台的更改。
- 适用于域控制器的新安装选项。
- 可简化 ADDS 安装的更新的安装向导。
- 改进的适用于 ADDS 的界面和管理选项。
- 改进的用于在企业内查找域控制器的工具。

现在，通过新的安装向导，所有相关的功能组合到了一起，从而，简化部署过程并节省部署时间。Windows Server 2008 中的无人参与安装从不要求响应任何用户界面提示，进一步简化了远程安装。这也使得可以在服务器核心安装上 ADDS。为确保新安装的 DNS 服务器正常运行，将基于所选的安装选项根据需要为 DNS 客户端设置、转发器和根提示自动配置 DNS。

通过对分支机构中的服务器精简初始部署并简化管理，Windows Server 2008 中提供的 ADDS 界面将节省 IT 管理时间。

1.10 高 可 用 性

确保关键任务应用程序始终可用是 IT 部门提供的一项关键服务，而且“高可用性”是 Windows Server 2008 提供的大量增强功能的一个关键主题。Windows Server 2008 中的故障转移群集、网络负载平衡和新的备份与还原功能共同为组织提供“高可用性”解决方案，从而确保所有用户可访问关键任务的应用程序、服务和信息。

1.10.1 故障转移群集

故障转移群集(以前称为服务器群集)是一组独立的计算机(如图 1-18 所示)，可协同工作以增强应用程序和服务的可用性。群集服务器(称为节点)通过物理电缆和软件连接。如果某个群集节点出现故障，则群集中的另一个节点会通过一个称为故障转移的过程取代出现故障的节点，从而确保用户感受到最低程度的服务中断。故障转移群集供需要为任务关键型服务和应用程序提供高可用性的 IT 专业人员使用。

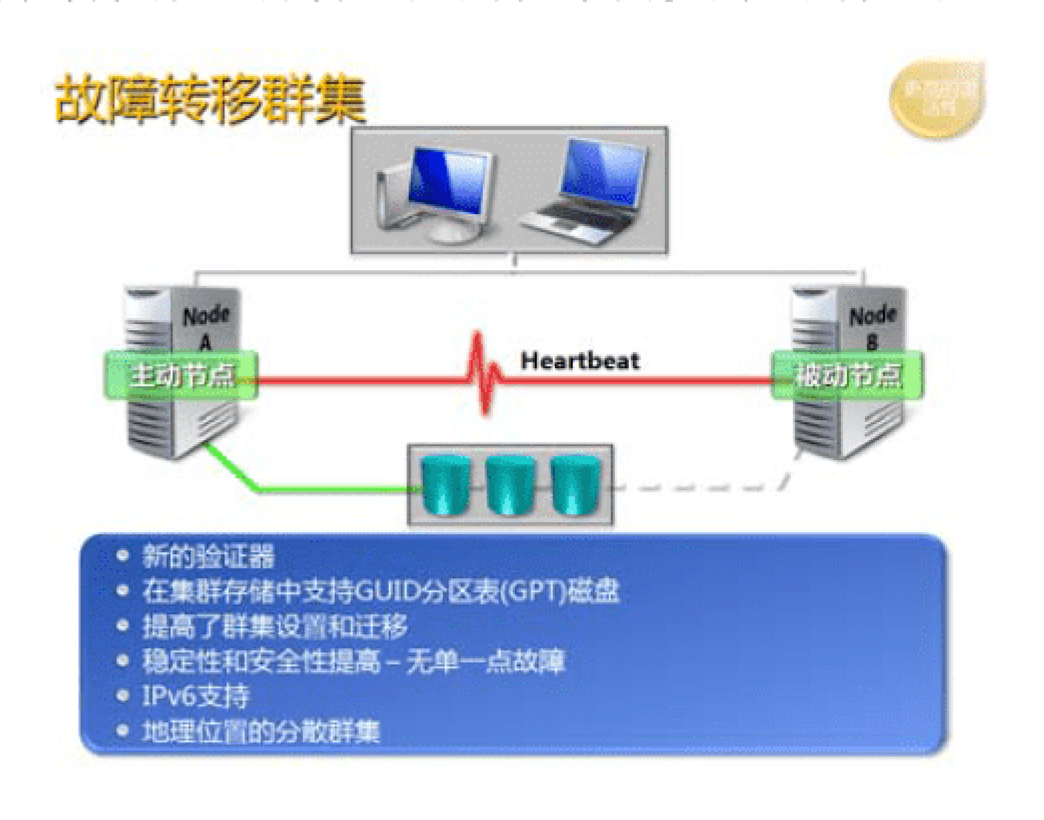


图 1-18 故障转移群集

在 Windows Server 2008 中，对故障转移群集的改进旨在简化群集、提高群集的安全性和稳定性。

在 Windows Server 2008 中，群集设置和配置已通过新的验证向导进行了简化，此向导使用户可以确认系统、存储和网络配置是否适用于群集。新的验证向导执行的部分测试所包括的内容如下。

- 节点测试：确认各个服务器是否在运行相同版本的操作系统，并且安装了相同的软件更新。
- 网络测试：确定计划的群集网络是否满足特定要求，如至少具有两个独立子网以实现网络冗余。
- 存储测试：分析是否对存储进行了正确配置，以便所有群集节点可以访问所有共享磁盘，并且满足指定的要求。

Windows Server 2008 支持在群集存储中使用全局唯一标识符或 GUID 分区表(GPT)磁盘。与主启动记录(Master Boot Record，MBR)磁盘不同，GPT 磁盘的分区大小超过 2TB 并具有内置冗余。与主启动记录(MBR)分区相比，GPT 具有更多的优点，因为它允许每个磁盘有多达 128 个分区、支持高达 18EB(注：1EB=1024PB= 1024^2 TB =1024^3 GB)的卷大小、允许将主分区表和备份分区表用于冗余，还支持唯一的磁盘

和分区 ID。

为了简化群集管理，管理界面已经过改进，使管理员可将精力集中在对应用程序和数据(而不是群集)的管理上。新的界面是基于任务的且更直观，用于指导管理员完成以前视为复杂操作的向导也对其提供支持。

与早期版本的服务器群集相比，Windows Server 2008 故障转移群集提供了更好的功能和可靠性。主要的改进包括以下内容。

- 动态添加磁盘资源：在资源联机时可以修改资源依赖关系，即管理员无须中断将使用某磁盘存储的应用程序即可添加该磁盘存储。
- 增强的数据存储性能和稳定性：故障转移群集与存储区域网络(Storage Area Network，SAN)或直接连接存储(Direct Attached Storage，DAS)通信时，将使用破坏性最小的命令，从而 SCSI 总线重置较少。磁盘从不会处于未受保护状态，这意味着降低了卷损坏的风险。故障转移群集还支持用于磁盘发现和恢复的改进方法。故障转移群集支持以下三种类型的存储连接：串行连接 SCSI(SAS)、iSCSI 和光纤通道。
- 更轻松的磁盘维护：“维护模式”得到了显著改进，因此管理员可以更轻松地运行工具对磁盘进行检查、修补、备份或还原，而对群集造成较小的破坏。

对于使用群集提供高可用性解决方案的管理员而言，Windows Server 2008 简化了群集的部署和管理，并且增强了性能和可靠性。

1.10.2　网络负载平衡

网络负载平衡(Network Load Balancing，NLB)是一种功能，用于在 NLB 群集中跨多个服务器为网络客户端和服务器应用程序分配负载。NLB 对于需要在一组服务器之间分发客户端请求的组织非常重要。NLB 尤其适用于确保随着工作负载的增加，添加更多服务器来扩展无状态应用程序(例如，在 Internet 信息服务(Internet Information Service，IIS)上运行的基于 Web 的应用程序)。NLB 允许随着负载的增加而添加其他服务器，从而提供了可伸缩性。NLB 通过允许用户轻松地替换不能正常运行的服务器提供可靠性。Windows Server 2008 中 NLB 的增强功能包括以下几项。

- 支持 IPv6：NLB 完全支持对所有通信使用 IPv6。
- 支持 NDIS 6.0：NLB 驱动程序已经过彻底的重新编写，以使用新的 NDIS6.0 轻型筛选模型。NDIS 6.0 保留了与早期 NDIS 版本的向后兼容性。NDIS 6.0 在设计方面的改进包括增强的驱动程序性能与可伸缩性和简化的 NDIS 驱动程序模型。
- WMI 增强功能：MicrosoftNLB 命名空间的 WMI 增强功能适用于 IPv6 及多个专用 IP 地址支持。
- MicrosoftNLB 命名空间中的类别：支持 IPv6 地址(也支持 IPv4 地址)。
- MicrosoftNLB_NodeSetting 类别：通过在 DedicatedIPAddresse 和 DedicatedNetMask 中进行指定，支持多个专用 IP 地址。
- ISA 服务器的增强功能：在客户端同时采用 IPv4 和 IPv6 进行通信的情况下，ISA 服务器可为每个 NLB 节点配置多个专用 IP 地址。IPv4 客户端和 IPv6 客户端都需要访问特定的 ISA 服务器来管理通信。ISA 还可为 NLB 提供 SYN 攻击和计时器停止运行通知(这类情况通常发生在计算机超载或感染 Internet 病毒时)。
- 支持每个节点有多个专用 IP 地址：NLB 完全支持为每个节点定义多个专用 IP 地址(以前，仅支持

每个节点有一个专用 IP 地址)，从而允许在不同的应用程序需要各自的专用 IP 地址时，一个 NLB 群集承载多个应用程序。

这些功能可支持新的行业标准、增强性能、加强互操作性、提高安全性以及提高部署和合并应用程序的灵活性。

1.10.3 Windows 备份

备份是 Windows Server 2008 的第三个关键部分，用来提供服务的高可用性。备份功能为安装该功能的服务器提供了一个备份和恢复解决方案。此功能引入了新的备份和恢复技术，取代了早期版本的 Windows 操作系统中提供的以前的备份功能。

备份功能可用于有效、可靠地保护整个服务器，而无须顾虑备份和恢复技术的复杂性。简单的向导可指导用户设置自动备份计划、创建手动备份(如果需要)以及恢复项目或所有卷。Windows Server 2008 中的备份可用于备份整个服务器或所选的卷。

备份功能使用卷影复制服务和程序块级备份技术来高效备份和恢复操作系统、文件和文件夹以及卷。在创建第一个完整备份后，备份功能通过仅保存自上次备份后更改的数据自动运行增量备份。与早期版本不同，管理员不用再担心手动计划完整备份和增量备份。

Windows Server 2008 改进和简化了还原功能。现在，通过选择要恢复项目的一个备份，然后选择要还原的项目，即可还原项目。还可选择还原特定文件或文件夹的所有内容。以前，对于增量备份，如果项目存储在增量备份中，则需将其从多个备份中手动还原。而现在，用户只需选择所要还原版本的备份日期即可。

Windows Server 2008 提供了构建高可用性的解决方案所需的备份和恢复解决方案，此方案可保护网络服务器中组织的数据和操作系统，同时可减轻确保正常备份关键任务数据的管理负担，还可加快数据恢复。

第 2 章　安装 Windows Server 2008

使用虚拟机 WMWare Workstation 搭建实战环境，本书的后续章节实战环境均基于虚拟机，例如，在虚拟机中安装 VMWare Tools，给系统做快照，克隆系统等常规设置。

在虚拟机环境中安装 Windows Server 2008 企业版，完成 Windows Server 2008 安装后的初始化配置，更改管理员密码，更改计算机名称，激活计算机。

安装 Windows Server Core 企业版，使用命令行完成初始化配置，更改计算机名称，更改 IP 地址、子网掩码和网关以及 DNS，激活 Windows Server Core。

使用 Windows PE 备份操作系统和还原操作系统，能够在系统启动失败的情况下，复制出系统目录下的重要数据，在忘记系统管理员密码的情况下，重设密码，能够恢复删除的文件。

关键词

- 了解 Windows Server 2008 有哪些版本
- 知道安装 Windows Server 2008 的硬件要求
- 能够使用虚拟机软件搭建学习环境
- 学会在虚拟机中安装 Windows Server 2008 企业版
- 学会 Windows Server 2008 安装完成后的初始化配置
- 学会在虚拟机中安装 Windows Server 核心版

2.1 Windows Server 2008 版本

1. Windows Server 2008 Standard Edition/ 32-bit Edition

该版本提供大多数服务器所需要的角色和功能，包括全功能的 Server Core 安装选项。

2. Windows Server 2008 Enterprise Edition/ 32-bit Edition

该版本在 Windows Server 2008 Standard Edition 的基础上提供更好的可伸缩性和可用性，添加了企业技术例如 Failover Clustering 与活动目录联合服务。

3. Windows Server 2008 Datacenter Edition / 32-bit Edition

该版本在 Windows Server 2008 Enterprise Edition 的基础上支持更多的内存和处理器，以及无限量使用虚拟镜像。

4. Windows Web Server 2008 / 32-bit

这是一个特殊版本的应用程序服务器，只包含 Web 应用，其他角色和 Server Core 都不存在。

5. Windows Server 2008 for Itanium-based Systems

该版本专为 Intel Itanium 64-bit 处理器设计，提供 Web 和应用程序服务器功能，根据平台支持的不同，部分角色和功能可能无法正确运行。

2.2 Windows Server 2008 对硬件的要求

1. 处理器

处理器性能不仅取决于处理器的时钟频率，而且取决于处理器内核数以及处理器缓存大小。以下是本产品对处理器的要求。

- 最低要求：1 GHz(对于 x86 处理器)或 1.4 GHz(对于 x64 处理器)
- 建议配置：2 GHz 或更高
- RAM

以下是本产品对 RAM 的要求。

- 最低要求：512 MB
- 建议配置：2 GB 或更多
- 最大(32 位系统)：4 GB(对于 Windows Server 2008 Standard)，或 64 GB(对于 Windows Server 2008 Enterprise 或 Windows Server 2008 Datacenter)
- 最大(64 位系统)：32 GB(对于 Windows Server 2008 Standard)，或 2 TB(对于 Windows Server 2008 Enterprise、Windows Server 2008 Datacenter 或面向基于 Itanium 系统的 Windows Server 2008)

2. 磁盘空间要求

以下是系统分区对磁盘空间的大致要求。对于基于 Itanium 的操作系统和基于 x64 的操作系统，这

些估计值将有所不同。如果通过网络安装系统，可能需要更多的磁盘空间。有关详细信息，可参阅 http://go.microsoft.com/fwlink/?LinkId=99285(可能为英文网页)。

- 最低要求：10 MB
- 建议配置：40 GB 或更多



注意：RAM 超过 16 GB 的计算机将需要更多的磁盘空间用于页面文件、休眠文件和转储文件。

- DVD-ROM 驱动器
- 超级 VGA (800×600)或更高分辨率的显示器
- 键盘和 Microsoft(R)鼠标(或其他兼容的指点设备)

2.3　虚　拟　机

在一台计算机上将硬盘和内存的一部分拿出来虚拟出若干台机器，每台机器可以运行单独的操作系统而互不干扰，这些“新”机器各自拥有自己独立的 CMOS、硬盘和操作系统，用户可以像使用普通机器一样对它们进行分区、格式化、安装系统和应用软件等操作，还可以将这几个操作系统联成一个网络。在虚拟系统崩溃之后可直接删除而不影响本机系统，同样本机系统崩溃后也不影响虚拟系统，可以下次重装后再加入以前做的虚拟系统。同时它也是唯一的能在 Windows 和 Linux 主机平台上运行的虚拟计算机软件。虚拟机软件不需要重开机，就能在同一台计算机使用好几个 OS，不但方便，而且安全。虚拟机在学习技术方面能够发挥很大的作用。



提示：常用的虚拟机软件有：VMware 6.02、微软公司的 Virtual PC 2007 和 Virtual Server 2005 R2。在 Windows Server 2008 中还内置了 Hyper-V 虚拟机。

2.4　Windows PE 介绍

Windows PreInstallation Environment(Windows PE)直接从字面上翻译就是“Windows 预安装环境”，微软在 2002 年 7 月 22 日发布，它的原文解释是：“Windows 预安装环境(Windows PE)是带有限服务的最小 Win32 子系统，基于以保护模式运行的 Windows XP Professional 内核。它包括运行 Windows 安装程序及脚本、连接网络共享、自动化基本过程以及执行硬件验证所需的最小功能。”换句话说，可把 Windows PE 看作是一个只拥有最少核心服务的 Mini 操作系统。微软推出这样一个操作系统当然是因为它拥有与众不同的系统功能，如果用一句话来解释，可以说与 Windows 9x/2000/XP/Vista 相比，Windows PE 的主要不同点就是：它可以自定义制作自身的可启动副本，在保证用户需要核心服务的同时保持最小的操作系统体积，同时它又是标准的 32 位视窗 API 的系统平台。

Windows PE 的作用如下。

1. 方便易用的启动工具盘

Windows PE 启动相当快捷，而且对启动环境要求不高；最可贵的是，虽然名为启动盘，其功能却几乎相当于安装了一个 Windows XP 的“命令行版本”。因此，对于个人计算机用户，只要将其刻录在一张光

盘上，便可放心地去解决初始化系统之类的问题；而对小型网络环境(如网吧等)用户来说，这一功能尤其实用。

2. 有趣的硬盘使用功能

Windows PE 提供如下几方面的硬盘使用功能。

- 替换系统文件。可以替换原始安装媒体上的损坏文件。例如，如果损坏的系统文件妨碍了计算机启动，则可以使用 Windows PE 来启动计算机，然后替换 Windows Vista 媒体中的损坏文件。
- 在重新安装 Windows 之前恢复数据。Windows PE 提供对 FAT 和 NTFS 文件系统的完全访问权限。在必须更换或重新格式化硬盘的情况下，可以首先用 Windows PE 启动计算机，然后将重要文件复制到另一个磁盘或共享文件夹中。应注意，利用“加密文件系统”(EFS)加密的文件不易被恢复。
- 运行诊断和配置工具。Windows PE 包括常用的命令行诊断工具。用户还可以在 Windows PE 内运行其他标准和自定义 Windows 故障排除工具。内置工具包括以下几种。
  - Diskpart：文本模式的命令解释程序，它允许用户通过命令提示符或脚本来管理磁盘、分区或卷。
  - Drvload：用户可使用 drvload 命令将设备驱动程序(如音频、视频和母板芯片集)添加到 Windows PE 映像中。在 Windows PE 已经启动后，还可使用 drvload 动态加载驱动程序。
  - Net Net：命令行工具，允许用户管理本地用户数据库、启动和停止服务以及连接共享文件夹。
  - Netcfg：该网络配置工具可配置网络访问。当将 Windows PE 作为自定义部署工具使用时，用户可能会使用 Netcfg 将网络设置作为部分启动脚本来手动配置。

2.5 实战：在虚拟机中安装 Windows Server 2008 企业版

任务描述

以下将演示如何安装 Windows Server 2008 企业版并完成初始化任务，能够联机激活操作系统。该操作在 VMWare Workstation 6.02 虚拟机中完成。

实战环境

- VMware 6.02 软件
- Windows Server 2008 安装光盘的 IOS 文件
- 能够连接到 Internet

实战目标

- 学会使用虚拟机
- 学会安装 Windows Server 2008 企业版操作系统
- 能够完成初始化任务配置
- 能够使用虚拟机软件创建快照
- 能够克隆操作系统

2.5.1 任务 1：创建虚拟机和配置

① 运行 VMWare Workstation 软件。单击 New Virtual Machine 按钮，然后单击“下一步”按钮。

② 如图 2-1 所示，在 New Virtual Machine Wizard 界面中，选中 Typical 单选按钮，单击“下一步”按钮。

③ 如图 2-2 所示，在 Select a Guest Operating System 界面中，选中 Microsoft Windows 单选按钮，Version 下拉列表框中选择 Windows Server 2008 选项，单击“下一步”按钮。

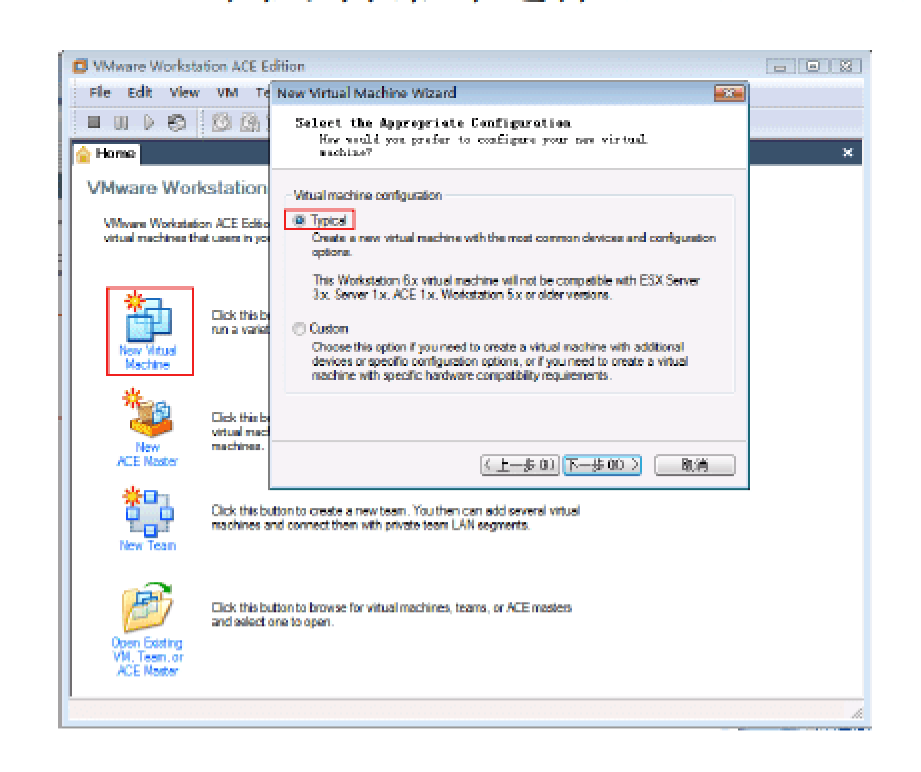


图 2-1　选择恰当的配置

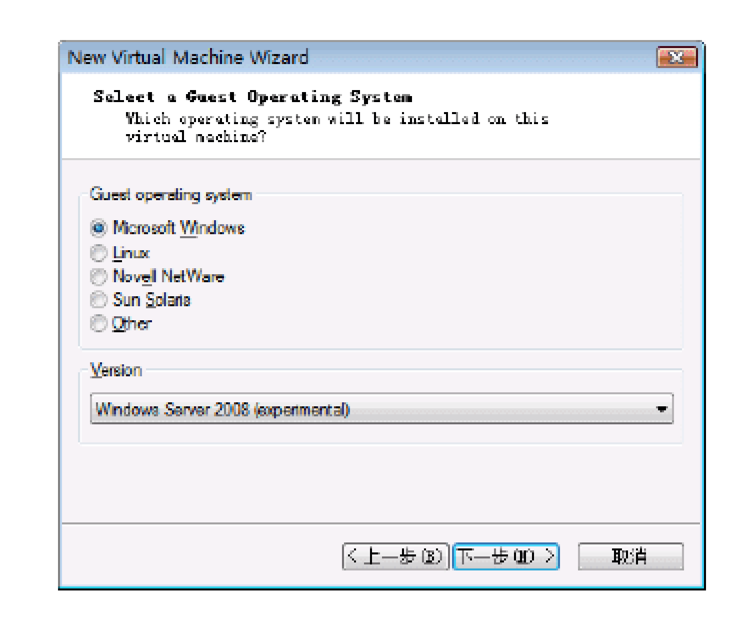


图 2-2　选择要安装的操作系统

④ 如图 2-3 所示，在出现的 Name the Virtual Machine 设置界面中，指定虚拟机的名称和存储位置。应注意存储位置所在的磁盘空间一定要有 10 GB 大小的空间，然后单击“下一步”按钮。

⑤ 如图 2-4 所示，在出现的 Network Type 设置界面中，设置网络类型，选中 Use bridged networking 单选按钮，单击“下一步”按钮。

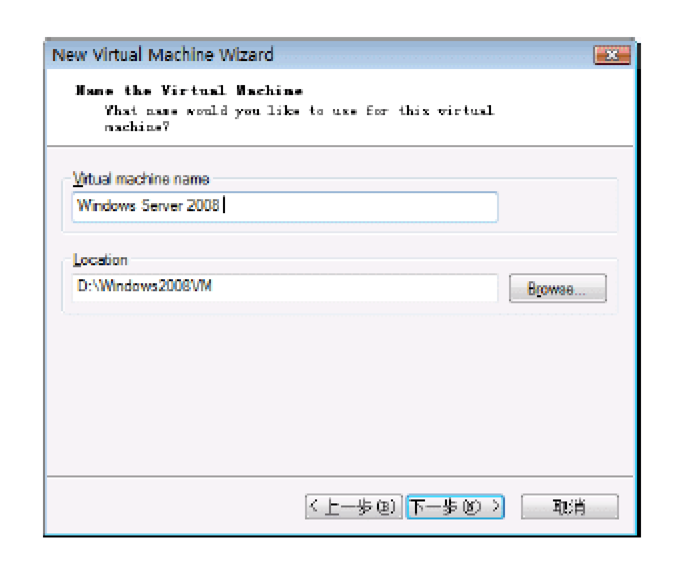


图 2-3　指定虚拟机的名称和位置

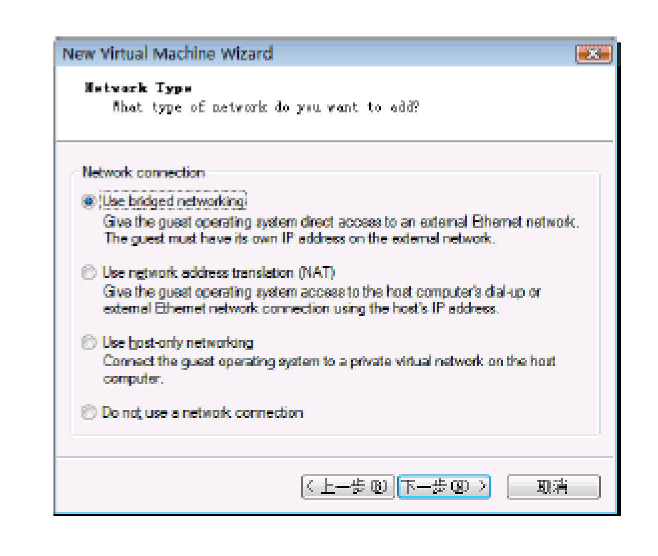


图 2-4　设置网络类型



提示：

■ bridge：如果你的主机在一个以太网上，这通常是让你的虚拟机访问该网络的最容易的方式。使用桥接网络，虚拟机在同一个物理以太网上显示为和主机一样的一台额外的计算机。显然，一台使用桥接网络的虚拟机可以使用在它桥接到的网络上的任何可用服务，包括：文件服务器、打印机、网关等。同样，使用桥接网络配置的任何物理计算机或者其他虚拟机可以使用该虚拟机的资源。

■ Hostonly：一种网络连接类型，虚拟机通过它在一个虚拟私有网络上被连接到主机操作系统，正常情况下，它对于主机外部是不可见的。可以在同一台主机上使用仅为主机网络配置的多台虚拟机并运行在同一个网络上。

■ nat 方式：如果想使用主机的拨号网络连接连接到 Internet 或者其他 TCP/IP 网络，而又不能在外部网络上给定虚拟机一个 IP 地址，这通常是让你的虚拟机访问该网络的最容易的方式。虚拟机在外部网络上不拥有它自己的 IP 地址；相反，在主机上安装有一个单独的私有网络。虚拟机从 VMware 虚拟 DHCP 服务器上获取该网络的一个地址。

⑥ 如图 2-5 所示，在出现的 Specify Disk Capacity 设置界面中，指定磁盘大小为 40 GB，完成向导。

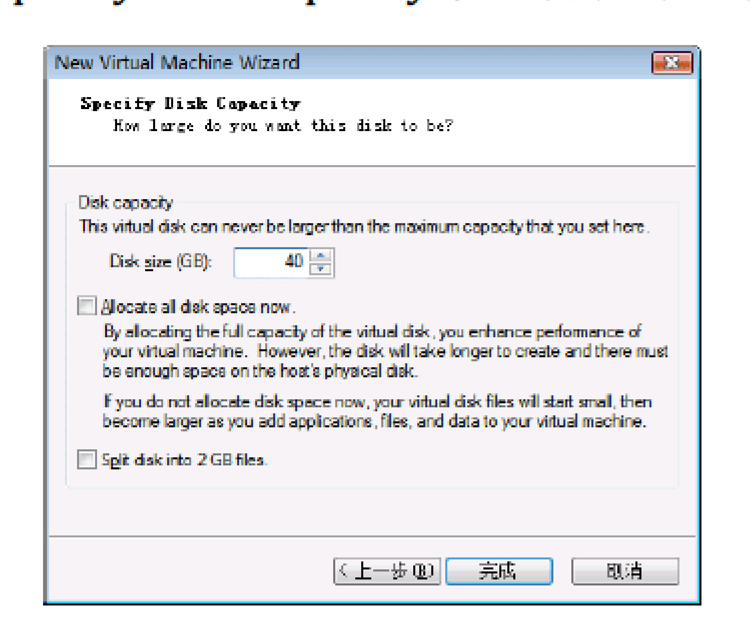


图 2-5　指定磁盘容量



提示：选择 4000 MB 的大小应该足够容纳用户操作系统和想在虚拟机中安装的所有软件，也为数据和今后的增长预留了空间。没有办法在以后增大这个数字，不过，如果你用完了这台虚拟机的空间，则可以使用配置编辑器安装额外的虚拟磁盘。

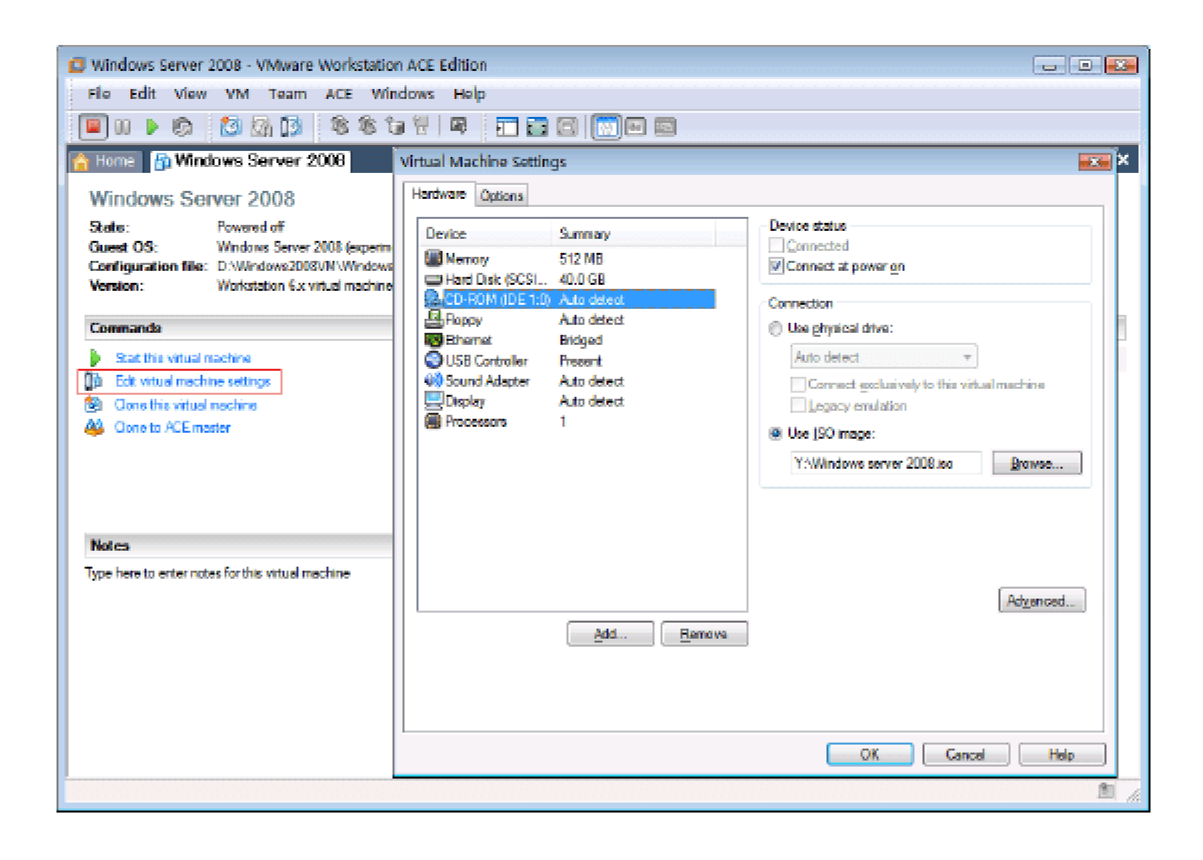
如果存放虚拟机的磁盘是 FAT 分区，会自动将磁盘文件分割为多个 2 GB 文件。

⑦ 如果选中 Allocate all disk space now 复选框，则立即占用磁盘 40 GB 的空间。

2.5.2　任务 2：在虚拟机中安装 Windows Server 2008 企业版

① 如图 2-6 所示，单击 Edit virtual machine settings 选项，设置光驱，选中 Use ISO image 单选按钮，指向 Windows Server 2008 安装盘的 ISO 文件，如果有安装光盘，就将安装盘放入光驱，选中 Use physical diver 单选按钮。

② 单击▷按钮，启动系统。会出现如图 2-7 所示的提示，这是因为物理机上没有软驱所致。单击 Yes 按钮，继续。



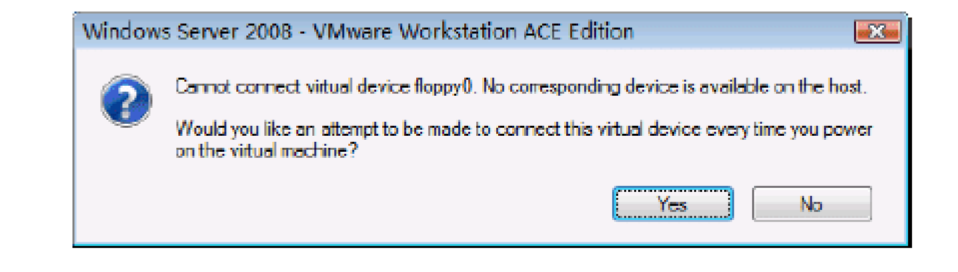


图 2-6　编辑虚拟机设置　　　　**图 2-7　提示不能连接虚拟软盘**

③ 如图 2-8 所示，在出现的 Windows 安装界面中，保持默认选择，单击“下一步”按钮。

④ 如图 2-9 所示，单击“现在安装”按钮。

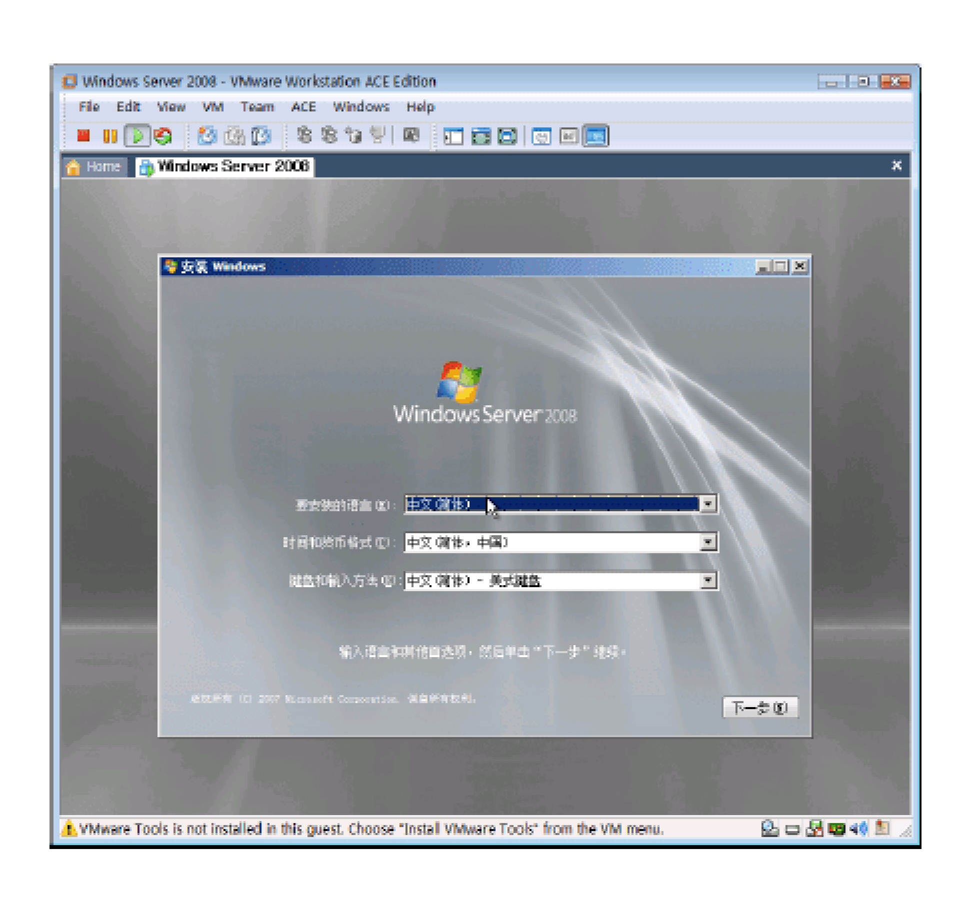


图 2-8　Windows 安装界面

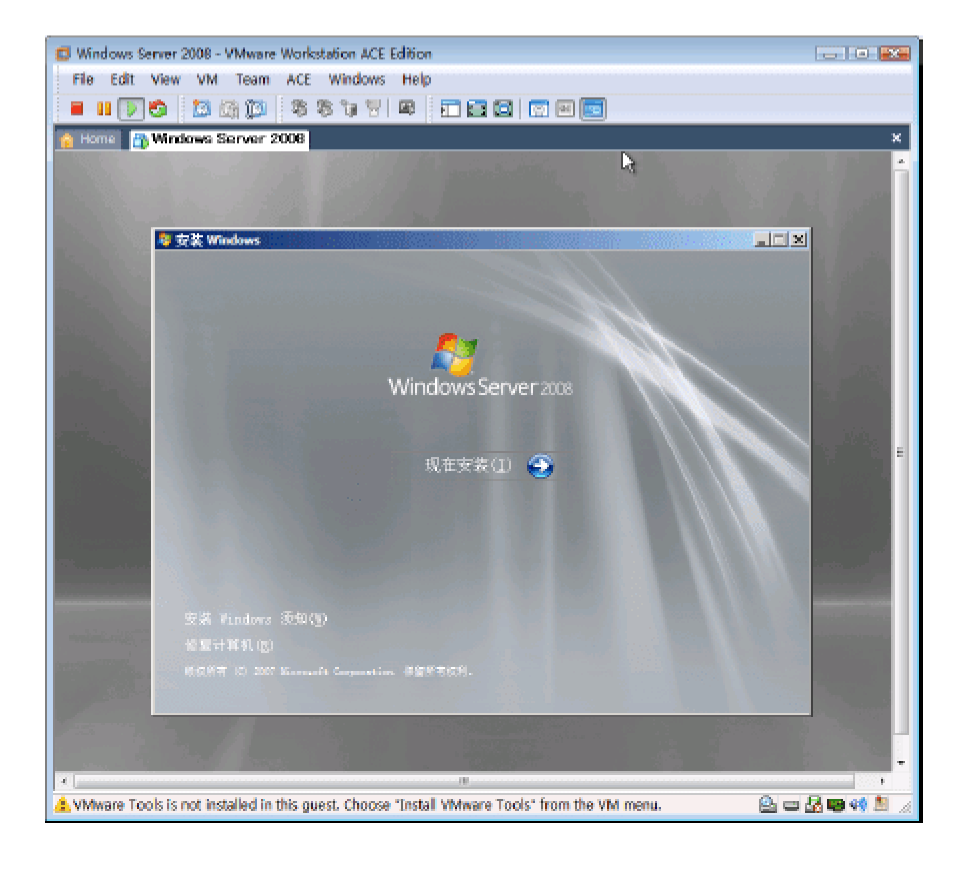


图 2-9　安装 Windows Server 2008

⑤ 如图 2-10 所示，选择要安装的操作系统版本 Windows Server 2008 Enterprise(完全安装)选项，单击“下一步”按钮。

⑥ 在出现的许可协议条款中，选中“我接受许可条款”单选按钮，单击“下一步”按钮。

⑦ 如图 2-11 所示，在出现的安装类型界面中，单击“自定义(高级)”按钮。

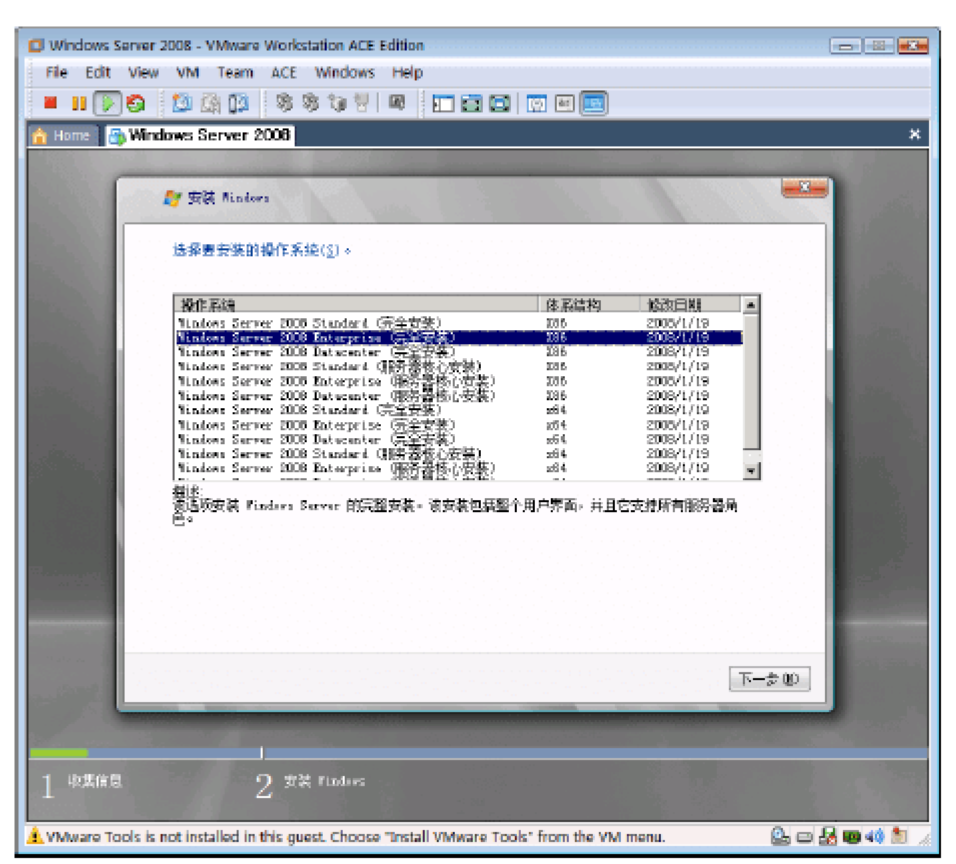


图 2-10　选择要安装的操作系统版本

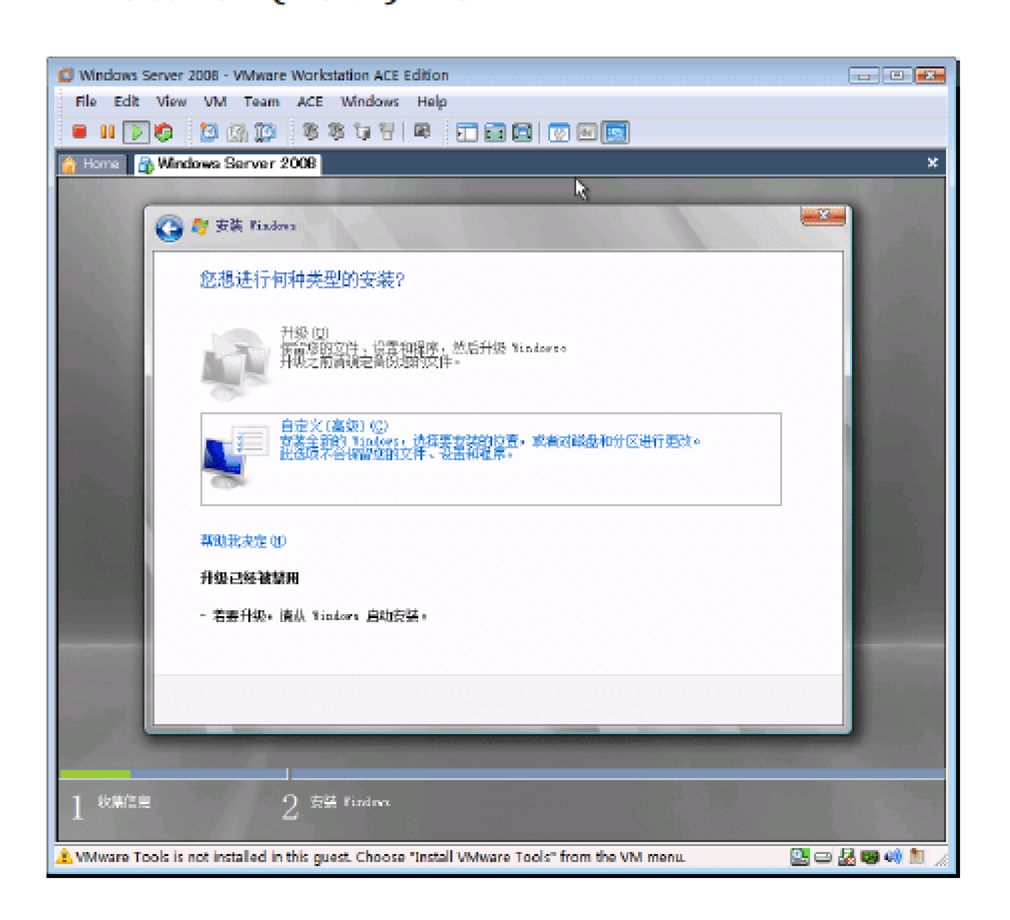


图 2-11　选择安装类型

⑧ 如图 2-12 所示，选择将操作系统安装在何处，如果直接单击“下一步”按钮，将整个磁盘创建成一个分区，并安装操作系统。单击“驱动器(高级)”按钮，可以创建磁盘分区，选择安装的位置。

⑨ 如图 2-13 所示，单击“新建”按钮，可以在这块硬盘上创建新的磁盘分区。

⑩ 如图 2-14 所示，指定分区大小为 20000 MB，单击“应用”按钮。

⑪ 如图 2-15 所示，选择刚才创建的分区，单击“下一步”按钮。复制文件，开始安装，自动重启，完成安装。

⑫ 剩下的时间你就可以去干别的事情了，等半小时左右系统即可装好。在此期间不需要像安装 Windows 其他版本一样，需要输入计算机名字、ProductID，设置管理员密码、IP 地址等信息，这些任务已经放到安装后的初始化任务中了。

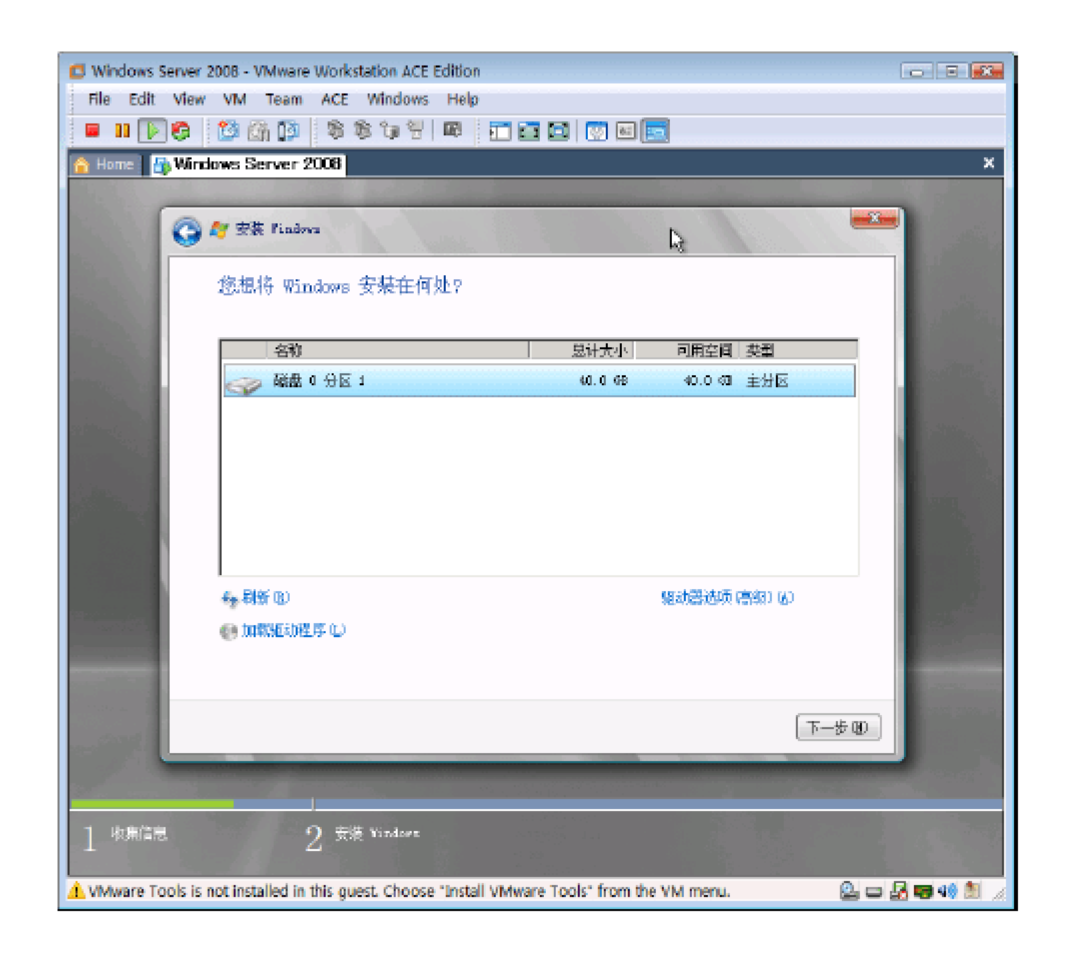


图 2-12 选择安装位置

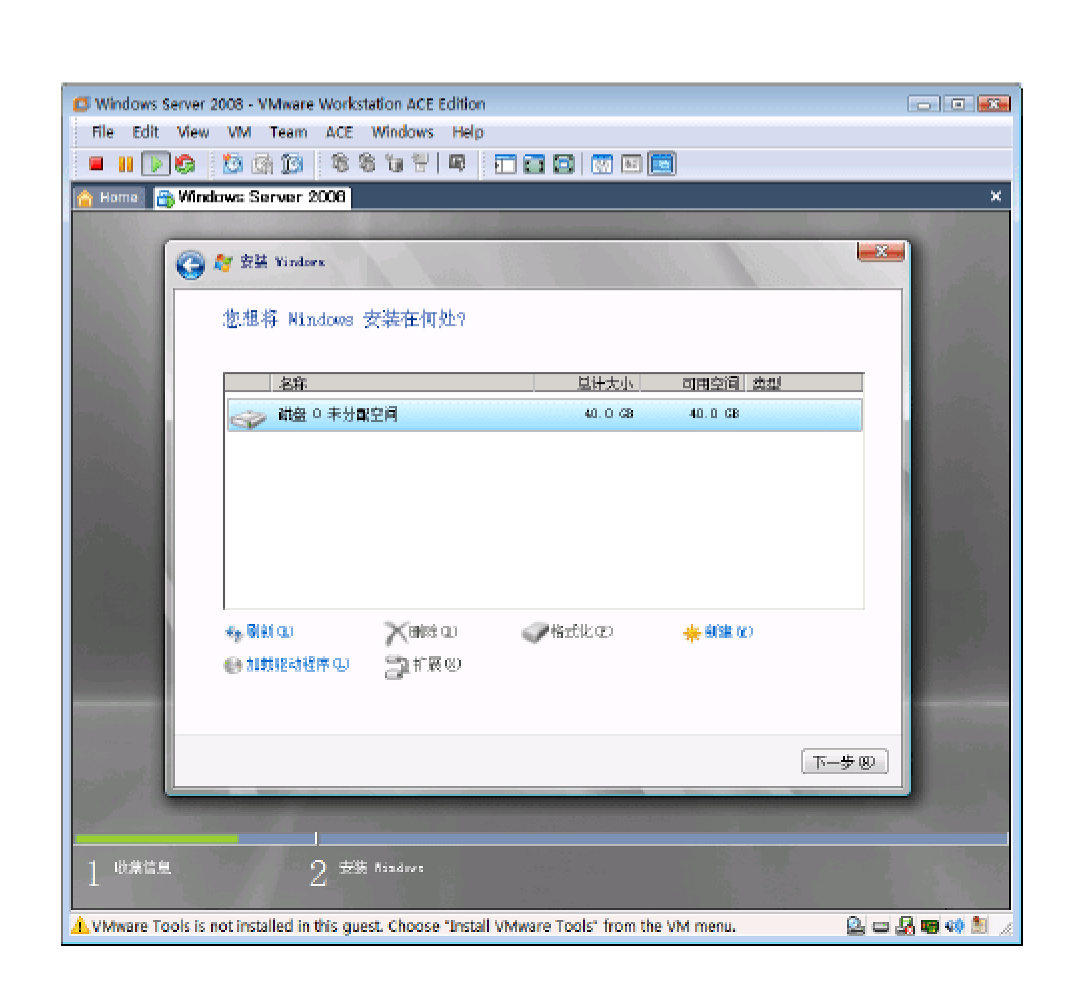


图 2-13 新建磁盘分区

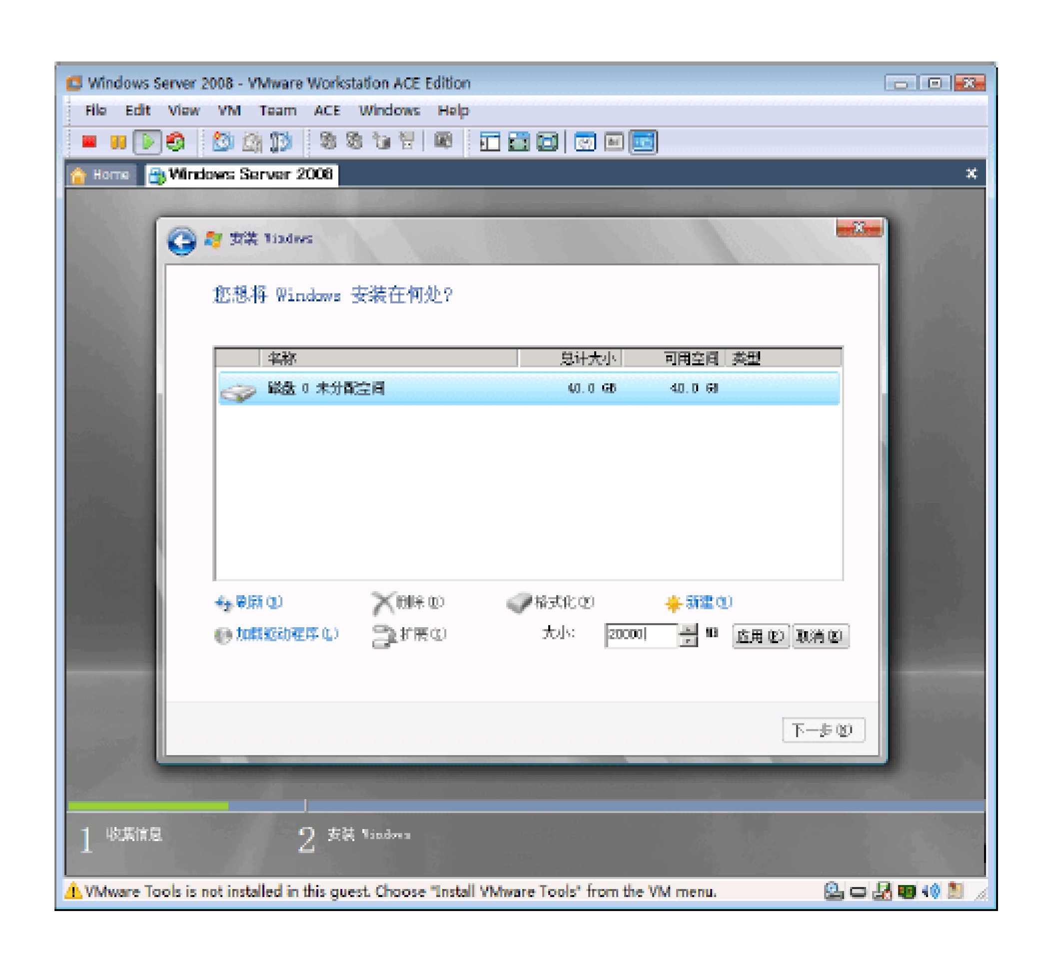


图 2-14 指定分区大小

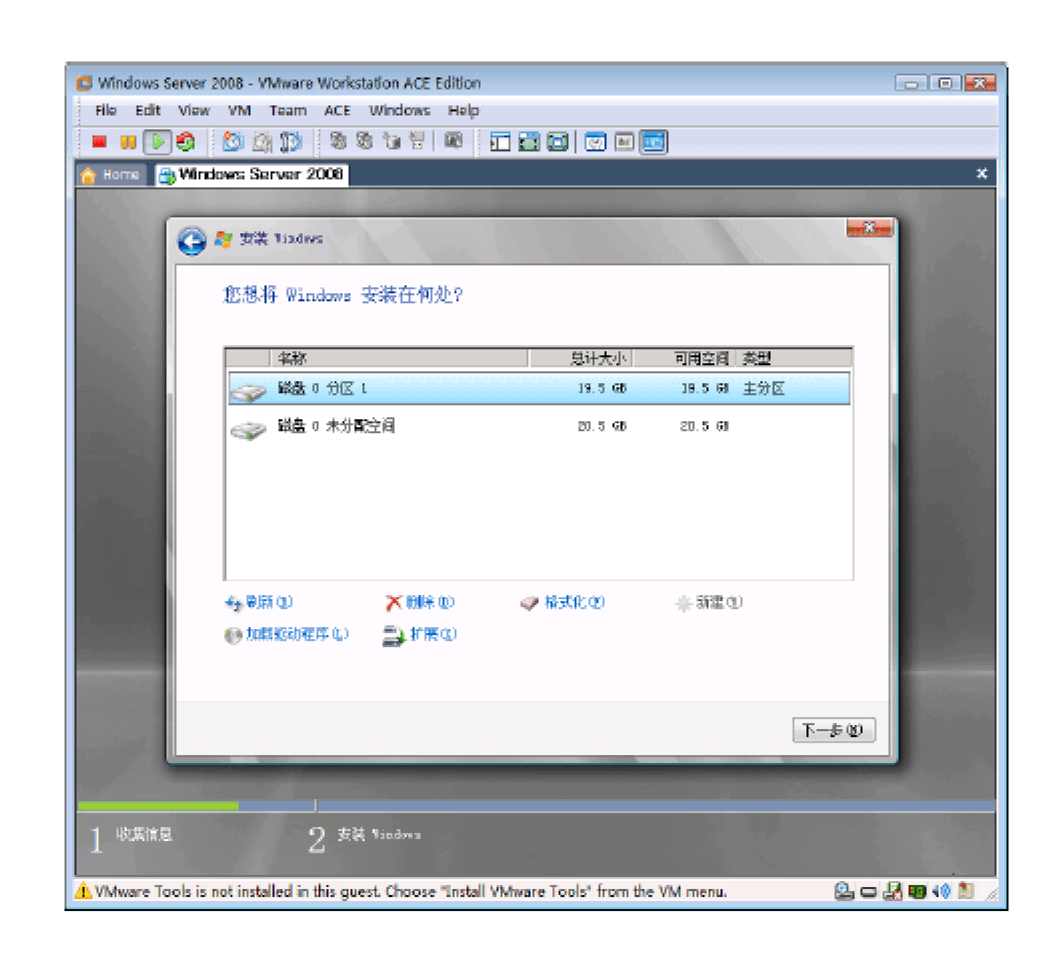


图 2-15 选择安装位置

2.5.3 任务 3：完成初始化任务

注意：登录虚拟机需要按 Ctrl+Alt+Insert 组合键，不能使用 Ctrl+Alt+Del 组合键。光标进入虚拟机窗口，要想将光标从虚拟机窗口中释放出来，需要按 Ctrl+Alt 组合键。

① 安装完成后，如图 2-16 所示，单击“确定”按钮，更改管理员密码。

② 如图 2-17 所示，输入新密码，单击按钮应用新密码。

注意：新密码必须满足长度复杂性要求。比如使用类似于这样的密码 p@ssw0rd，这个密码中有字符、数字和特殊符号，还必须是 7 位以上。这样的密码才能满足策略要求，如果是单纯的字符或数字，不管你的密码设置多长都不会满足密码策略要求。

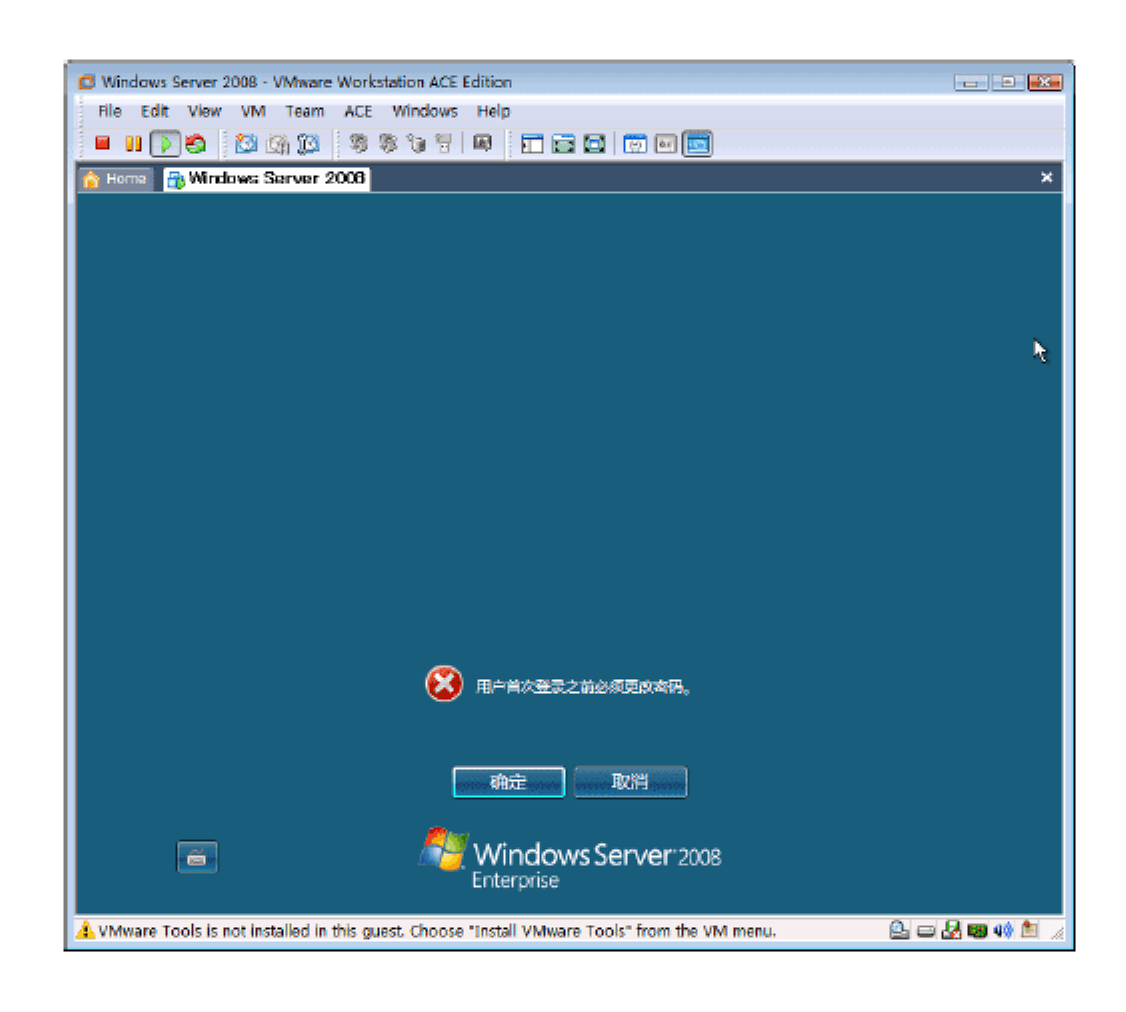


图 2-16　用户首次登录之前必须更改密码

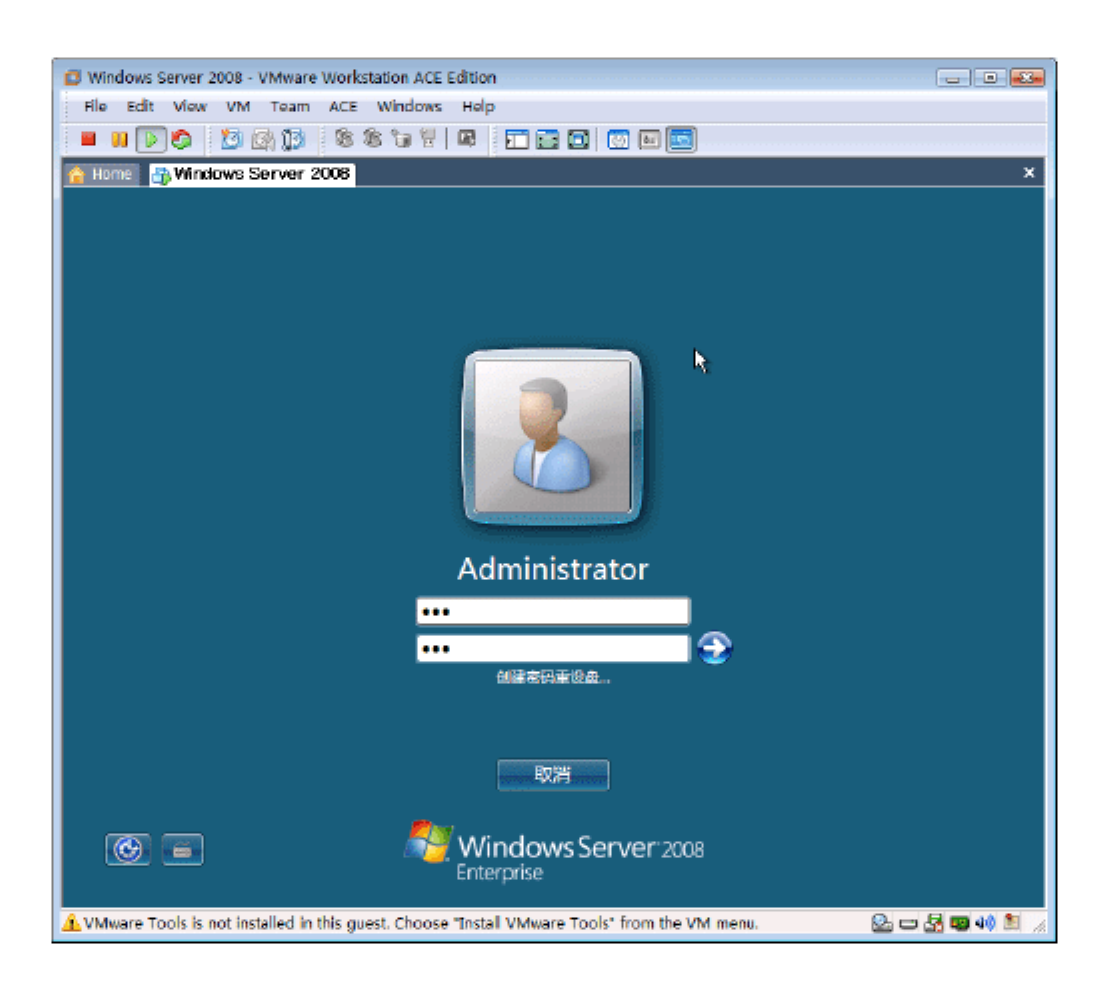


图 2-17　输入新密码

③　首次登录后，出现初始任务界面如图 2-18 所示。如果没有出现该界面，选择“开始”→“运行”命令，输入 oobe，单击“确定”按钮，也可以打开初始化任务。

④　如图 2-18 所示，单击“配置网络”选项，在出现的“网络连接”对话框中右击“本地连接”选项，在弹出的“本地链接 状态”对话框中单击“属性”按钮，如图 2-19 所示。



图 2-18　初始化任务对话框

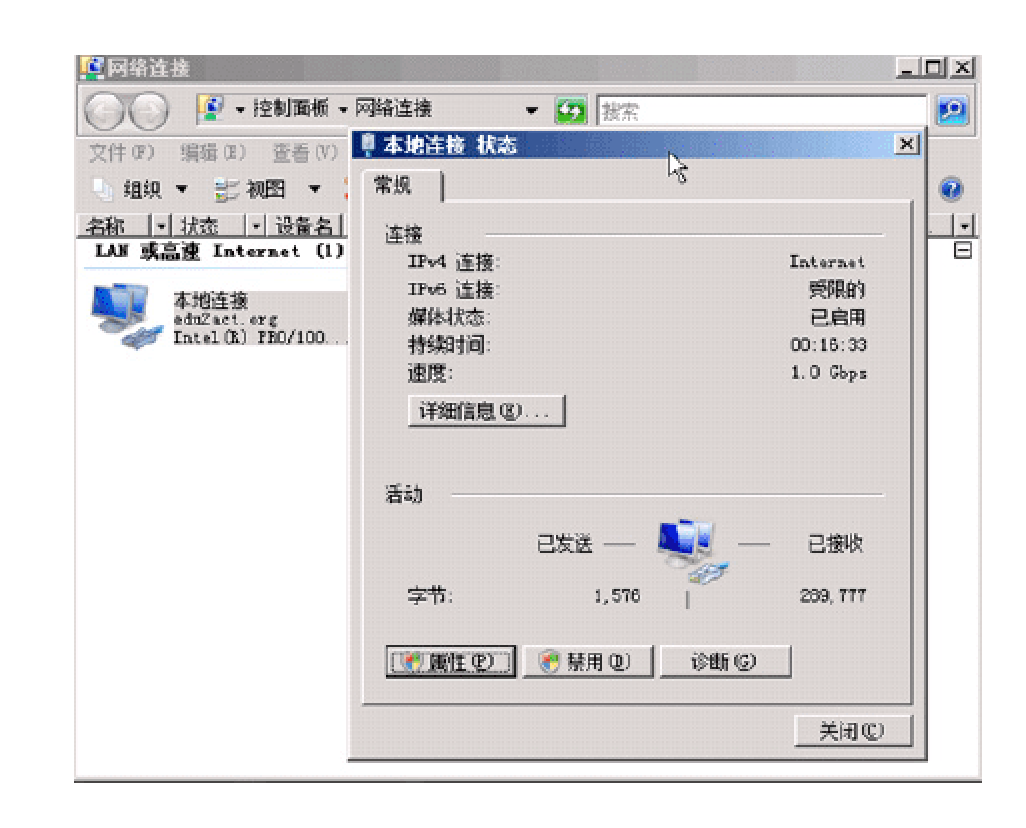


图 2-19　更改本地连接

⑤　在如图 2-20 所示的对话框中，取消对 IPv6 的支持，选中“Internet 协议版本 4(TCP/IPv4)”，单击“属性”按钮。

⑥　如图 2-21 所示，出现“Internet 协议版本 4(TCP/IPv4)属性”对话框，更改 IP 地址，单击“确定”按钮。

⑦　单击初始化任务界面上的“提供计算机名和域”选项，如图 2-22 所示，出现“系统属性”对话框，单击“更改”按钮。

⑧　如图 2-23 所示，在出现的“计算机名/域更改”对话框中，输入计算机名称，单击“确定”按钮。

⑨　提示重启才能生效，最后单击“立即重启”按钮即可。



图 2-20　选中 TCP/IP 协议

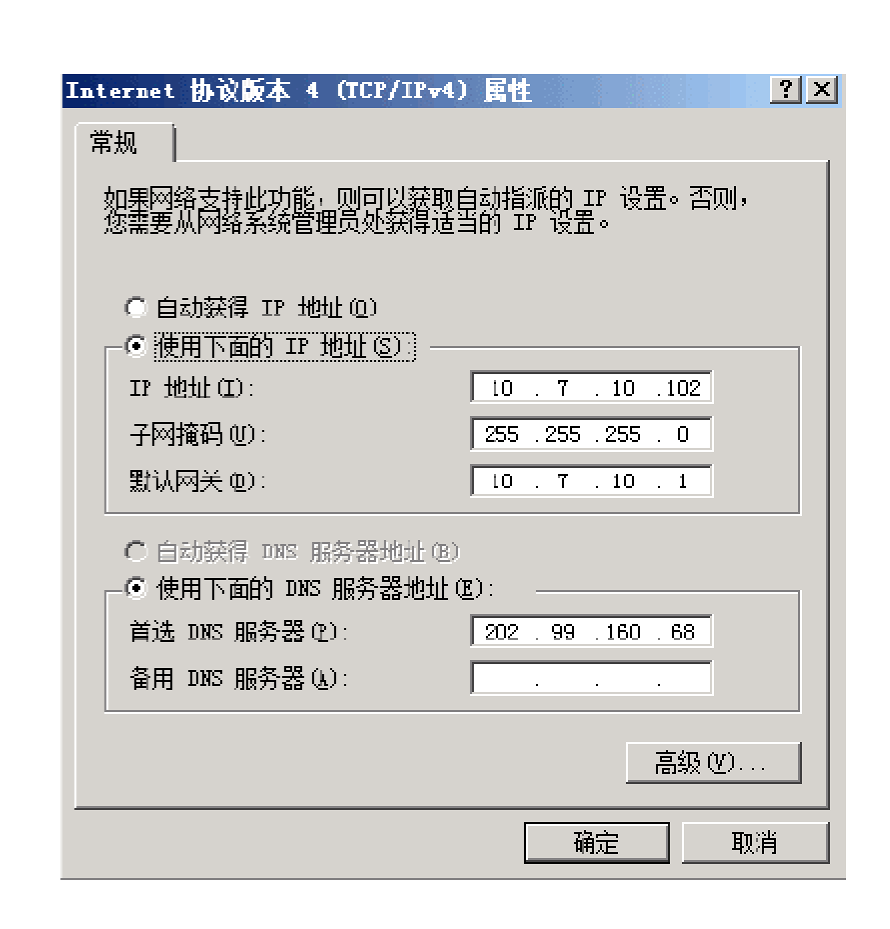


图 2-21　更改 TCP/IP 属性



图 2-22　更改系统属性

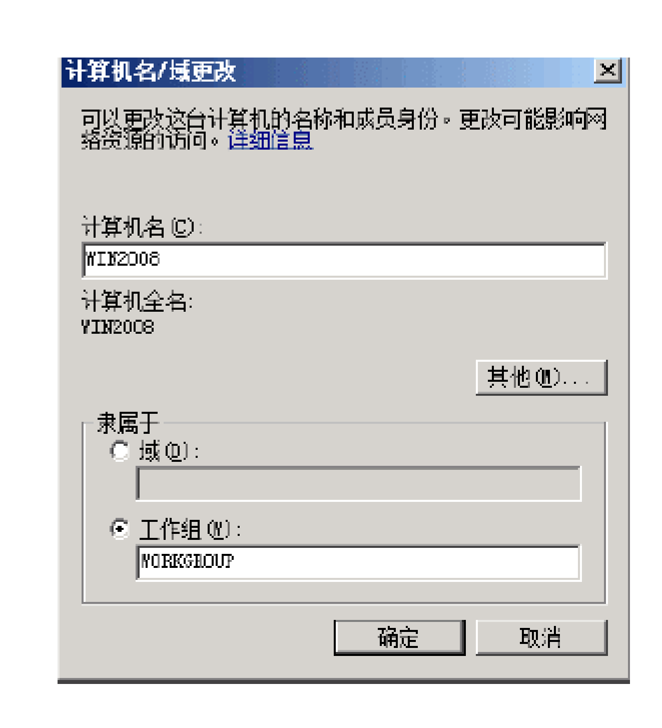


图 2-23　更改计算机名和所属的工作组

2.5.4　任务 4：配置系统自动更新和启用远程桌面

运行 Windows Update 后，可以对产品上市后发现的故障进行修正、下载新增加的功能，对 Windows 进行更新。

什么是远程桌面

当某台计算机开启了远程桌面连接功能后用户就可以在网络的另一端控制这台计算机了，通过远程桌面功能可以实时地操作这台计算机，在上面安装软件，运行程序，所有的一切都如同直接在该计算机上操作。这就是远程桌面的最大功能，通过该功能网络管理员可以在家中安全地控制单位的服务器，而且由于该功能是系统内置的，所以比其他第三方远程控制工具使用更方便、更灵活。

启用远程桌面，不需要购买远程桌面连接许可，但只能同时建立两个远程桌面会话。

① 按 Ctrl+Alt+Insert 组合键，输入账户和密码登录虚拟机。

② 在初始化任务中，单击“下载并安装更新”选项，在出现的 Windows Update 界面中单击“更改

设置”选项，如图 2-24 所示。

③ 如图 2-25 所示，选中“自动安装更新(推荐)”单选按钮，在“推荐更新”中选中“下载、安装或通知更新时包括推荐的更新”复选框，单击“确定”按钮。

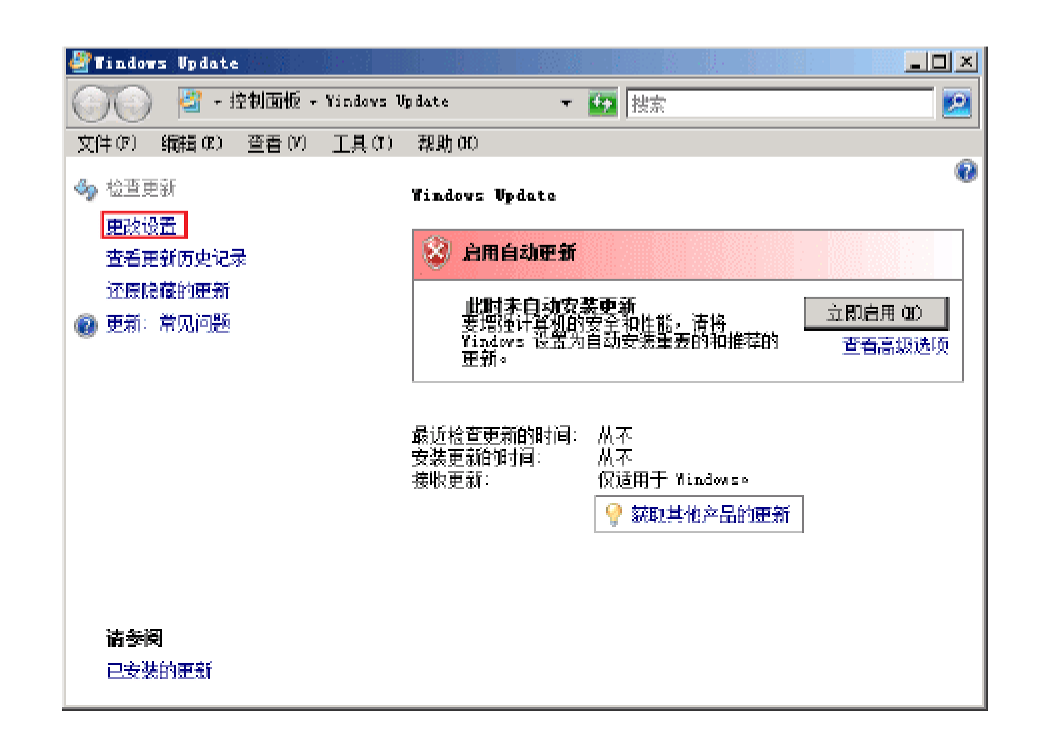


图 2-24　配置 Windows Update

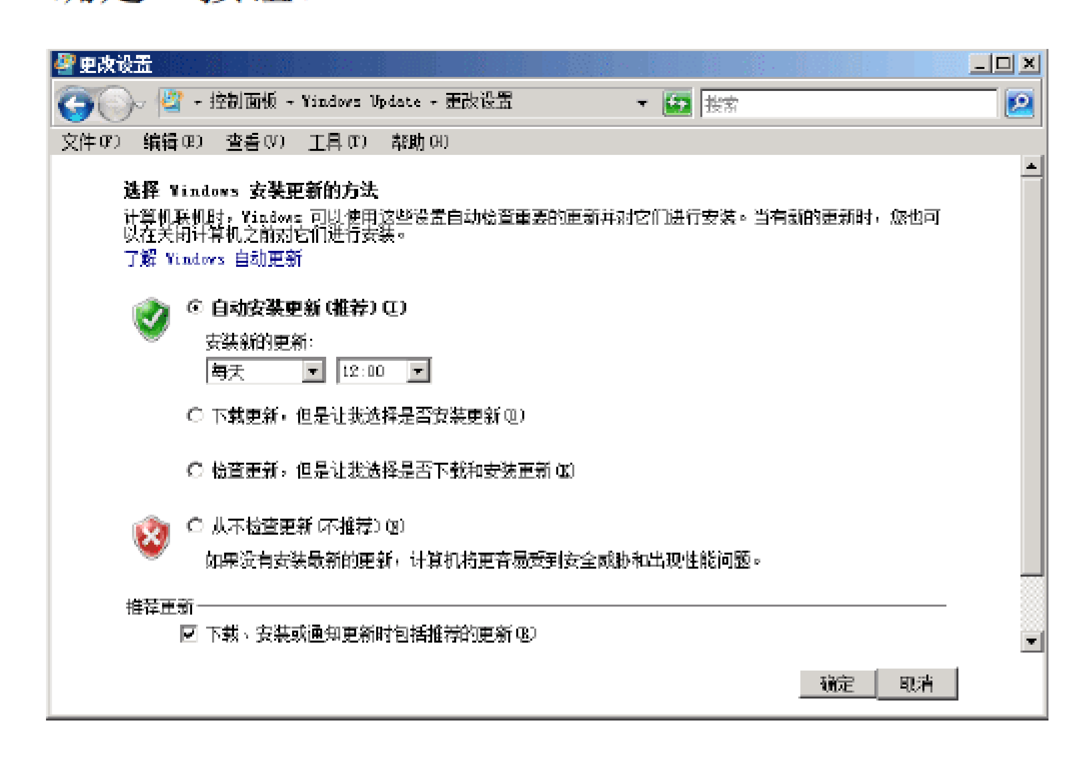


图 2-25　设置自动更新

④ 如图 2-26 所示，单击“查看更新历史记录”选项，单击“查看可用更新”按钮。

⑤ 如图 2-27 所示，在初始化对话框中，单击“启用远程桌面”按钮，在随后打开的对话框中选中“允许运行任意版本远程桌面的计算机连接(较不安全)”单选按钮。单击“确定”按钮，远程计算机即可使用远程桌面客户端连接到该服务器。



图 2-26　查看更新历史记录

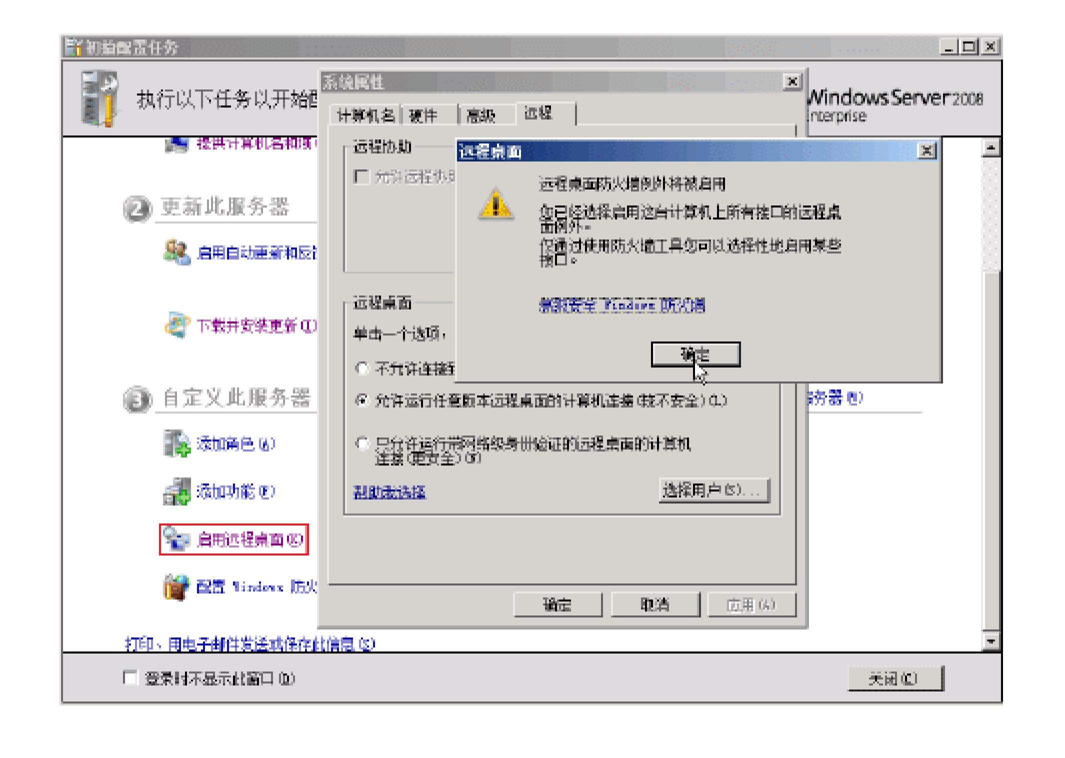
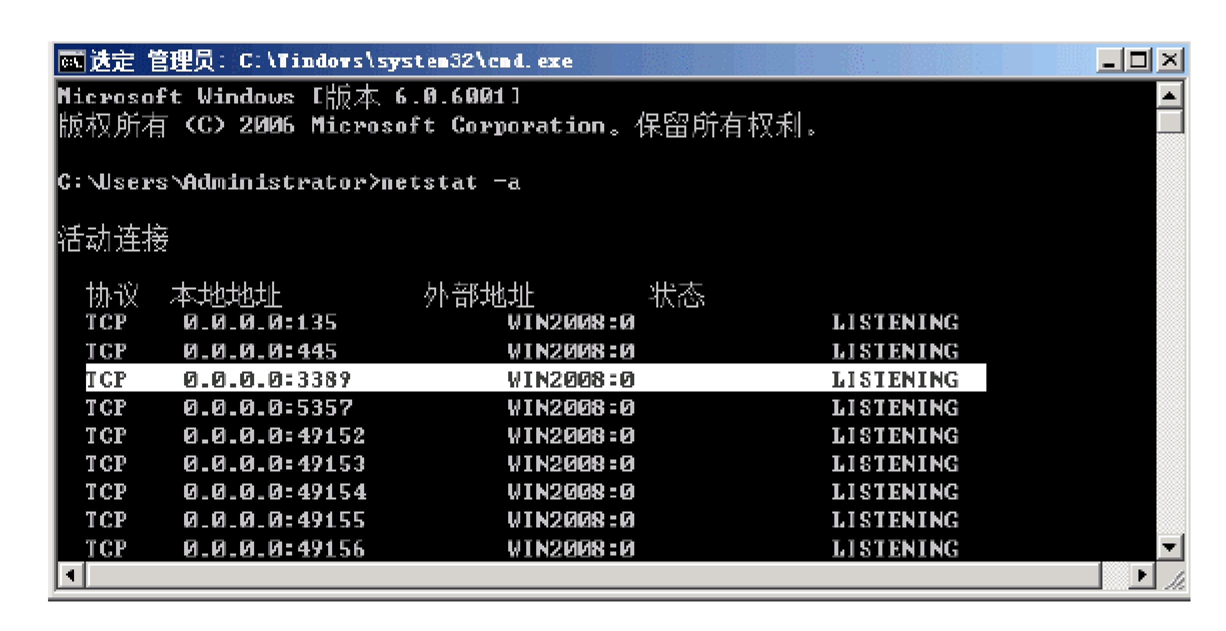


图 2-27　启用远程桌面

⑥ 选择“开始”→“运行”命令，输入 cmd，打开命令行，输入 netstat –a，如图 2-28 所示。此时能够查看启用远程桌面后打开的端口 3389，表明其他计算机可以通过远程桌面连接过来了。



```
选定 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netstat -a

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135       WIN2008:0       LISTENING
  TCP    0.0.0.0:445       WIN2008:0       LISTENING
  TCP    0.0.0.0:3389      WIN2008:0       LISTENING
  TCP    0.0.0.0:5357      WIN2008:0       LISTENING
  TCP    0.0.0.0:49152     WIN2008:0       LISTENING
  TCP    0.0.0.0:49153     WIN2008:0       LISTENING
  TCP    0.0.0.0:49154     WIN2008:0       LISTENING
  TCP    0.0.0.0:49155     WIN2008:0       LISTENING
  TCP    0.0.0.0:49156     WIN2008:0       LISTENING
```

图 2-28　查看远程桌面打开的端口

⑦ 如图 2-29 所示，在命令行中输入 net user han a1!/add，创建用户。

⑧ 输入 net localgroup “remote desktop users” han/add，将用户加入到远程桌面组。

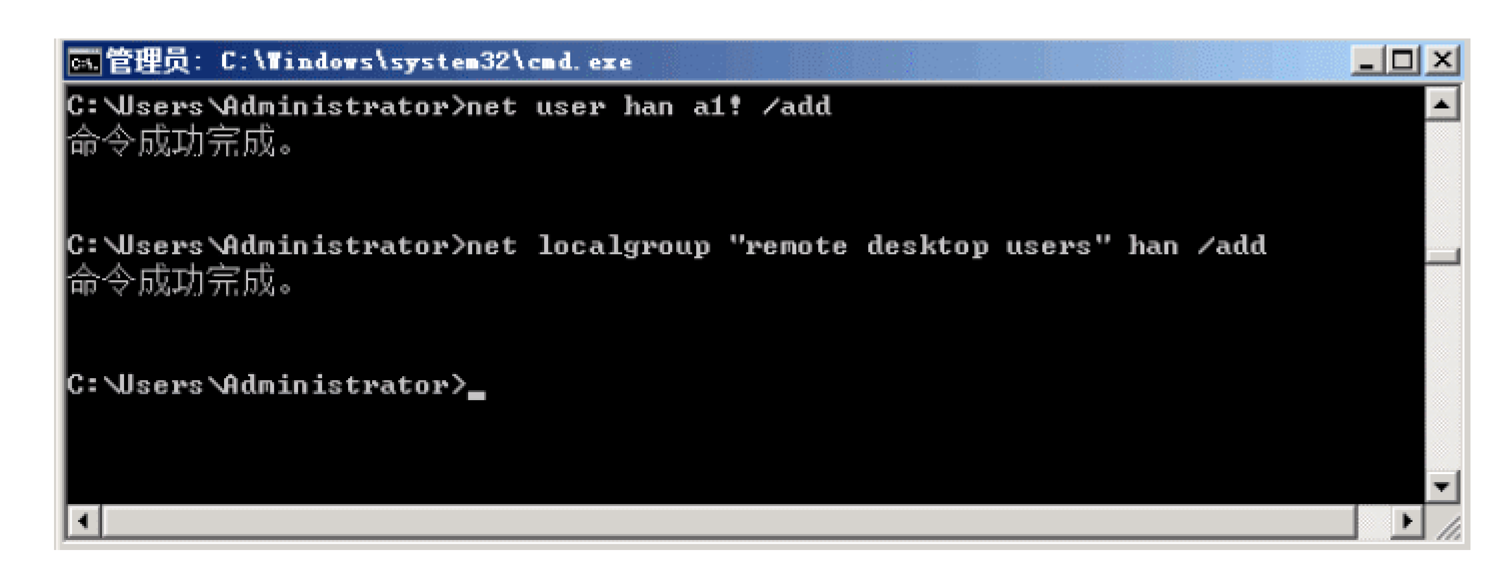


图 2-29　创建用户将用户添加到 remote desktop users 组



注意：将用户添加到 remote desktop users 组，该用户就能使用远程桌面连接到该服务器了。

⑨ 选择“开始”→“运行”命令，输入 mstsc，打开远程桌面客户端。

⑩ 如图 2-30 所示，输入该计算机的 IP 地址或计算机名，单击“连接”按钮。

⑪ 如图 2-31 所示，在出现的“Windows 安全”对话框中，输入账户 han，密码 a1!。这样即可使不同的用户同时登录同一台计算机了。

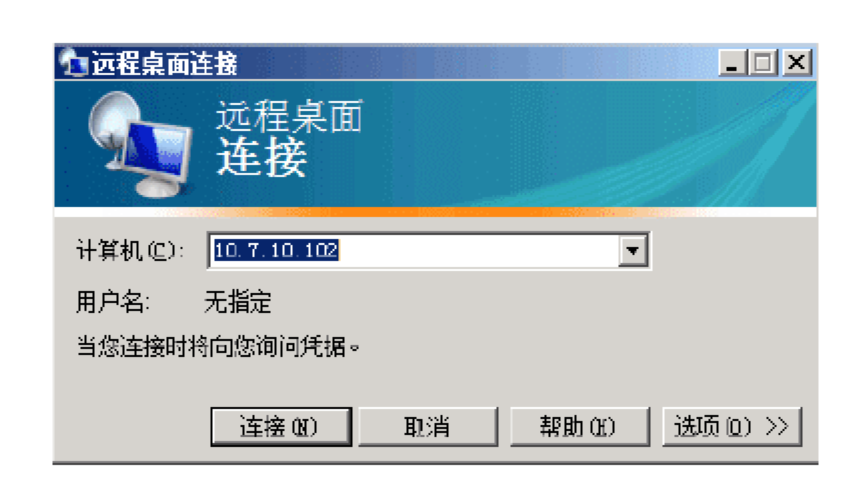


图 2-30　远程桌面客户端

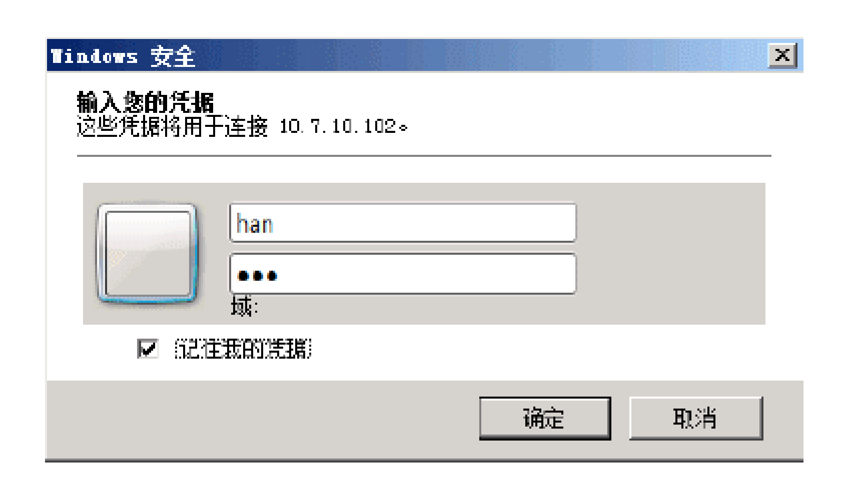


图 2-31　远程桌面网络级身份验证

2.5.5　任务 5：配置 Windows 防火墙和激活服务器

防火墙可以是软件，也可以是硬件，它能够检查来自 Internet 或网络的信息，然后根据防火墙设置阻止或允许这些信息通过计算机。

防火墙有助于防止黑客或恶意软件(如蠕虫)通过网络或 Internet 访问计算机。防火墙还有助于阻止计算机向其他计算机发送恶意软件。

图 2-32 所示，显示了防火墙的工作方式。



图 2-32　Windows 防火墙的工作方式

1. 配置 Windows 防火墙

① 单击初始化任务界面上“配置 Windows 防火墙”选项。

② 如图 2-33 所示，在出现的“Windows 防火墙”对话框中，单击“更改设置”按钮，可以启用防火墙，也可关闭防火墙。

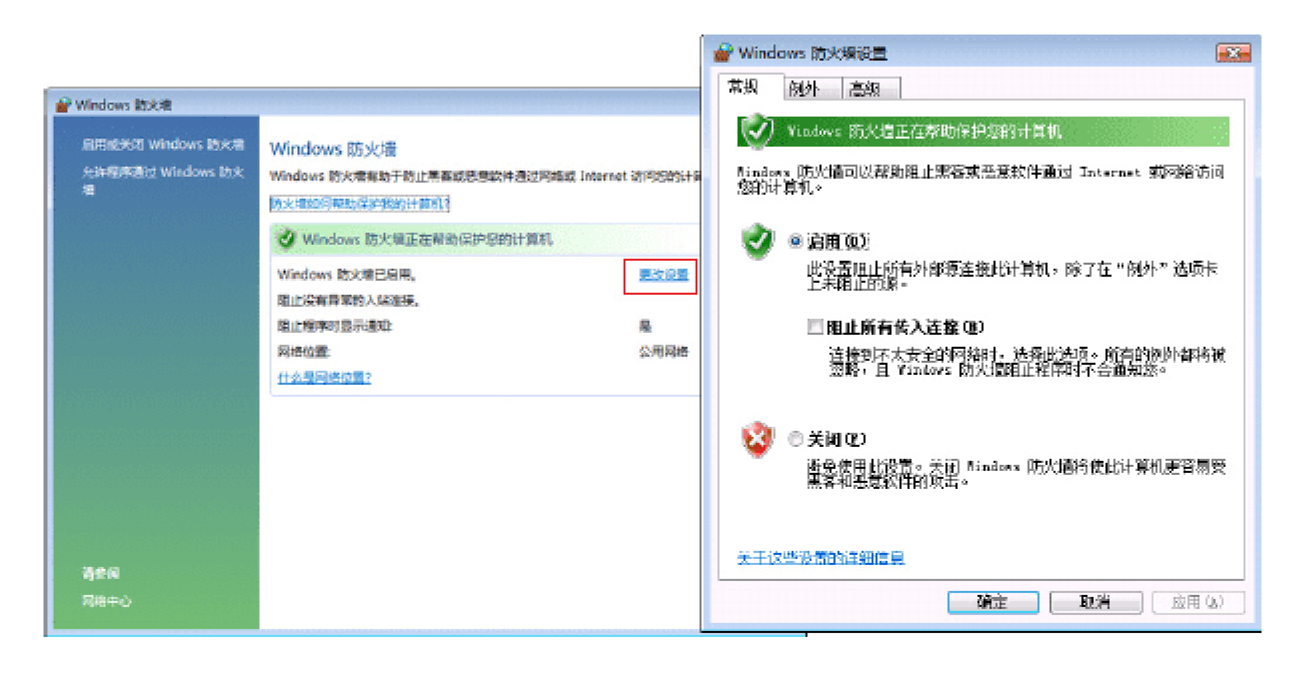


图 2-33　Windows 高级防火墙

③　如图 2-34 所示，切换到“例外”选项卡，可以开放一些端口，或允许一些程序侦听网络请求。比如用户的计算机对外提供 Web 服务，则需要单击“添加端口”指定协议以及服务所侦听的端口，单击“更改范围”按钮，可以指定哪些地址段的计算机能够访问该端口。

注意： 常用端口，包括访问共享文件夹使用 TCP 的 445 端口，远程桌面协议(RDP)使用 TCP 的 3389 端口，访问 Web 站点(HTTP)使用 TCP 的 80 端口，访问安全的 Web 站点(HTTPS)使用 TCP 的 443 端口，域名解析(DNS)使用 UDP 的 53 端口，发送电子邮件(SMTP)使用 TCP 的 25 端口，接收电子邮件(POP3)使用 TCP 的 110 端口。

④　如果用户不知道应用程序用的是什么端口，单击“添加程序”按钮，可以直接添加应用程序，如图 2-35 所示。

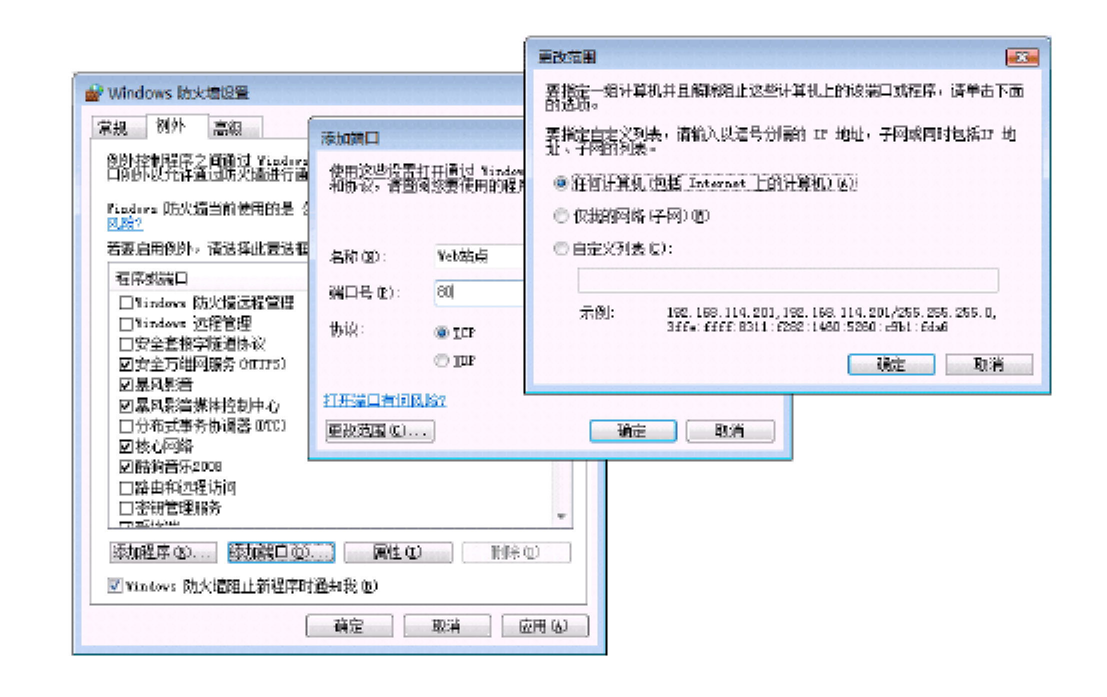


图 2-34　设置防火墙例外

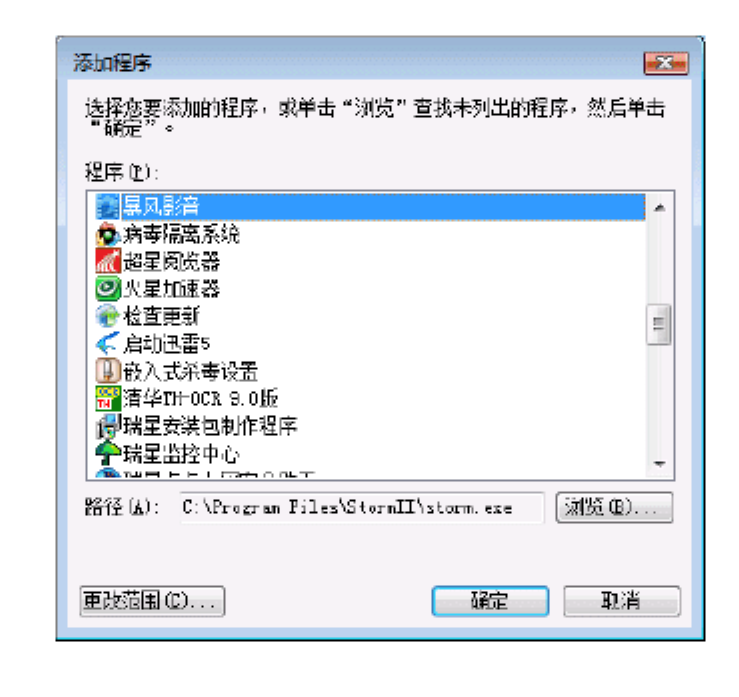


图 2-35　添加应用程序

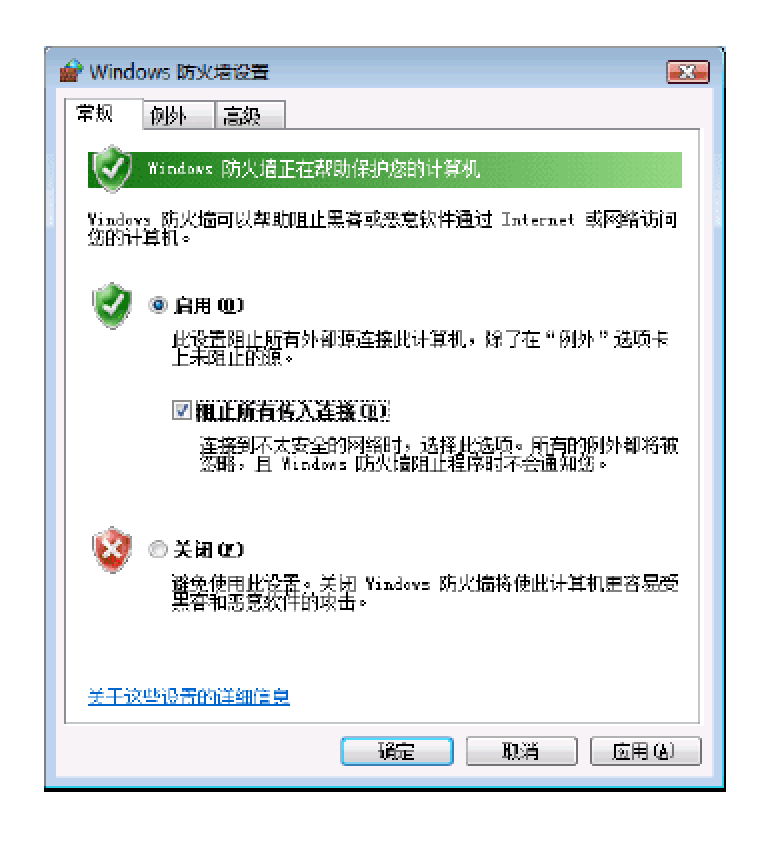


提示： 如图 2-36 所示如果选择了启用防火墙，也选中了“阻止所有传入连接”复选框，则其他计算机主动访问这台计算机的请求都将被拒绝，这就相当于该计算机在网上隐身了，但并不影响这台计算机访问其他计算机。

⑤　切换到“高级”选项卡，如果用户的计算机有多个网卡，可以指定防火墙应用到哪些网卡。如图 2-37 所示“本地连接”将不应用防火墙设置。

2. 激活服务器

新安装的 Windows Server 2008 必须激活才能正常使用。下面将演示如何联机激活 Windows Server 2008。操作系统必须连接到 Internet 才能联机激活。



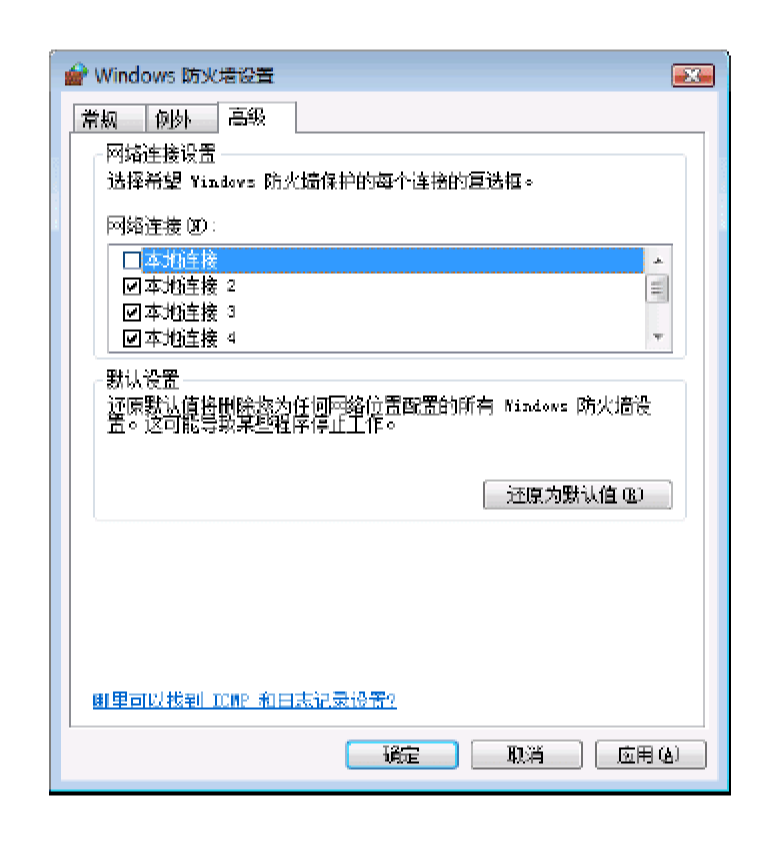


图 2-36　Windows 防火墙设置　　　图 2-37　设置防火墙应用到的网络连接

3. 联机激活 Windows Server 2008

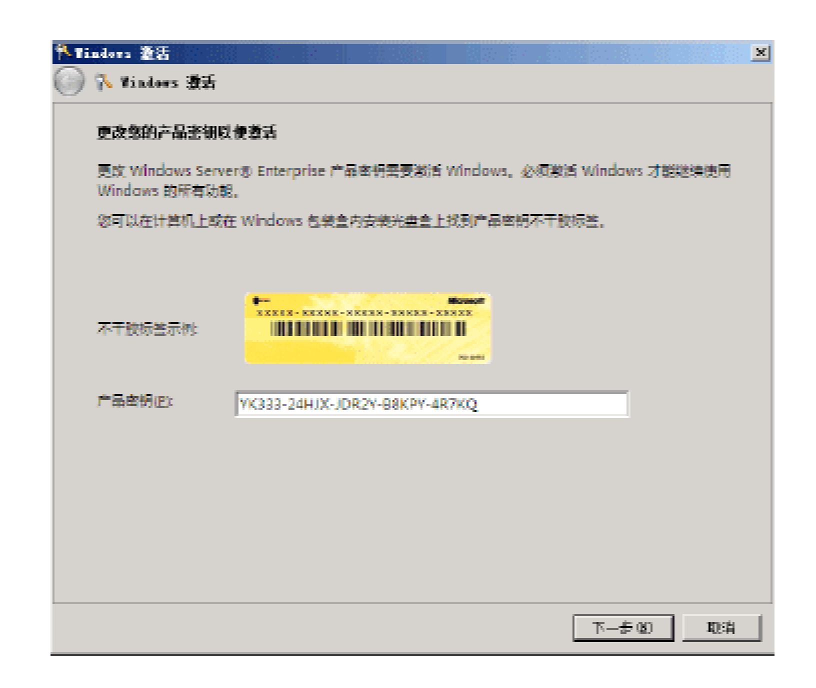
① 如图 2-38 所示，选择“开始”→“控制面板”→“系统”命令，弹出“系统”对话框，单击“更改产品密钥”按钮。



图 2-38　更改产品密钥

② 如图 2-39 所示，输入产品密钥，单击“下一步”按钮。

③ 如图 2-40 所示，提示联机激活成功！



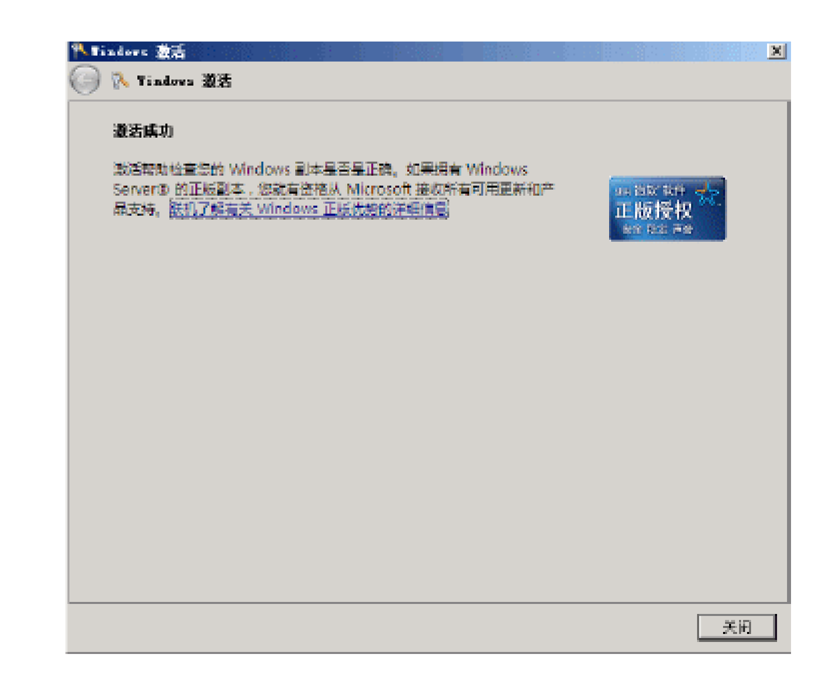


图 2-39　输入产品密钥　　　图 2-40　激活成功

2.6 实战：虚拟机的常规设置

任务描述

学会虚拟机的常规设置，包括安装 VMWare Tools，给虚拟机添加/删除硬件，调整虚拟机的内存大小，调整网卡连接状态，能够为安装好的系统做快照，能够克隆新的操作系统。

实战环境

在虚拟机中装好 Windows Server 2008 企业版的操作系统。

实战目标

- 学会安装 VMWare Tools
- 添加/删除硬件
- 调整内存大小
- 设置网卡连接状态
- 能够给配置好的系统做快照
- 能够使用装好的系统克隆新的系统

2.6.1 任务 1：安装 VMWare Tools

在构造一台虚拟机时，这个安装过程是第一步并且是唯一必需的一步。但是，VMware 强烈建议你在每一台虚拟机中完成操作系统安装之后立即安装 VMware Tools 套件。在客户操作系统中安装 VMware Tools 非常重要。如果你不安装 VMware Tools，虚拟机中的图形环境被限制为 VGA 模式图形(640×480，16 色)。

使用 VMware Tools，SVGA 驱动程序被安装。VMware Workstation 支持最高 32 位显示和高显示分辨率，显著提升总体的图形性能。

工具包中的其他工具通过支持下面的增强让用户更方便地使用虚拟机。注意，只有正在运行 VMware Tools 时，这些增强才可用。

- 在主机和客户机之间同步时间



注释：只有当用户在客户操作系统中设置时钟为一个比在主机中设置的时间更早的时间时，才可以在客户和主机操作系统之间同步时间。

- 自动捕获和释放光标
- 在主机和客户机之间或者从一台虚拟机到另一台虚拟机进行复制和粘贴操作
- 改善的网络性能

① 按 Ctrl+Alt+Insert 组合键，输入账户和密码登录虚拟机。

② 如图 2-41 所示，选择 VM→Install VMware Tools 命令。

③ 如图 2-42 所示，在出现的“自动播放”对话框中单击“运行 setup.exe”，安装完后重启。如果没有出现对话框，单击虚拟机的光驱，也可出现该对话框。

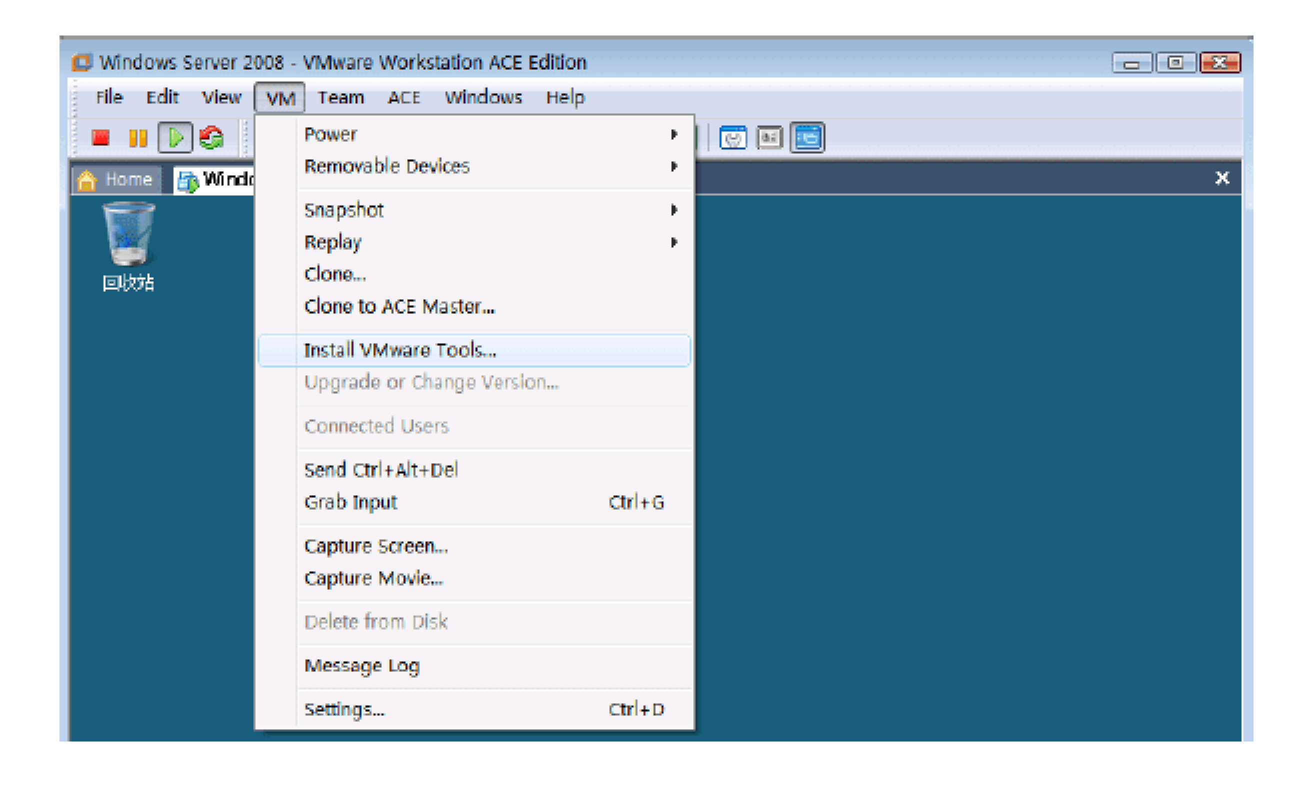




图 2-41　安装 VMware Tools

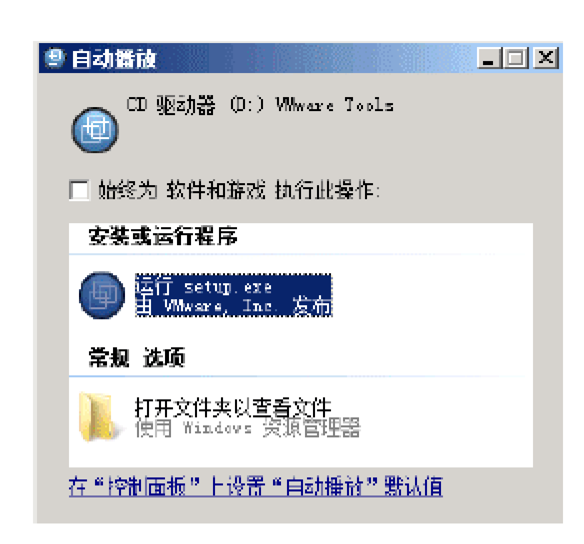


图 2-42　直接运行安装程序



提示：自动捕获和释放光标，不需要按 Ctrl+Alt 组合键。

④　验证安装 VMware Tools 后的效果，在主机和客户机之间或者从一台虚拟机到另一台虚拟机进行复制和粘贴操作，如图 2-43 所示，可以将物理机的文件直接拖进虚拟机系统中。

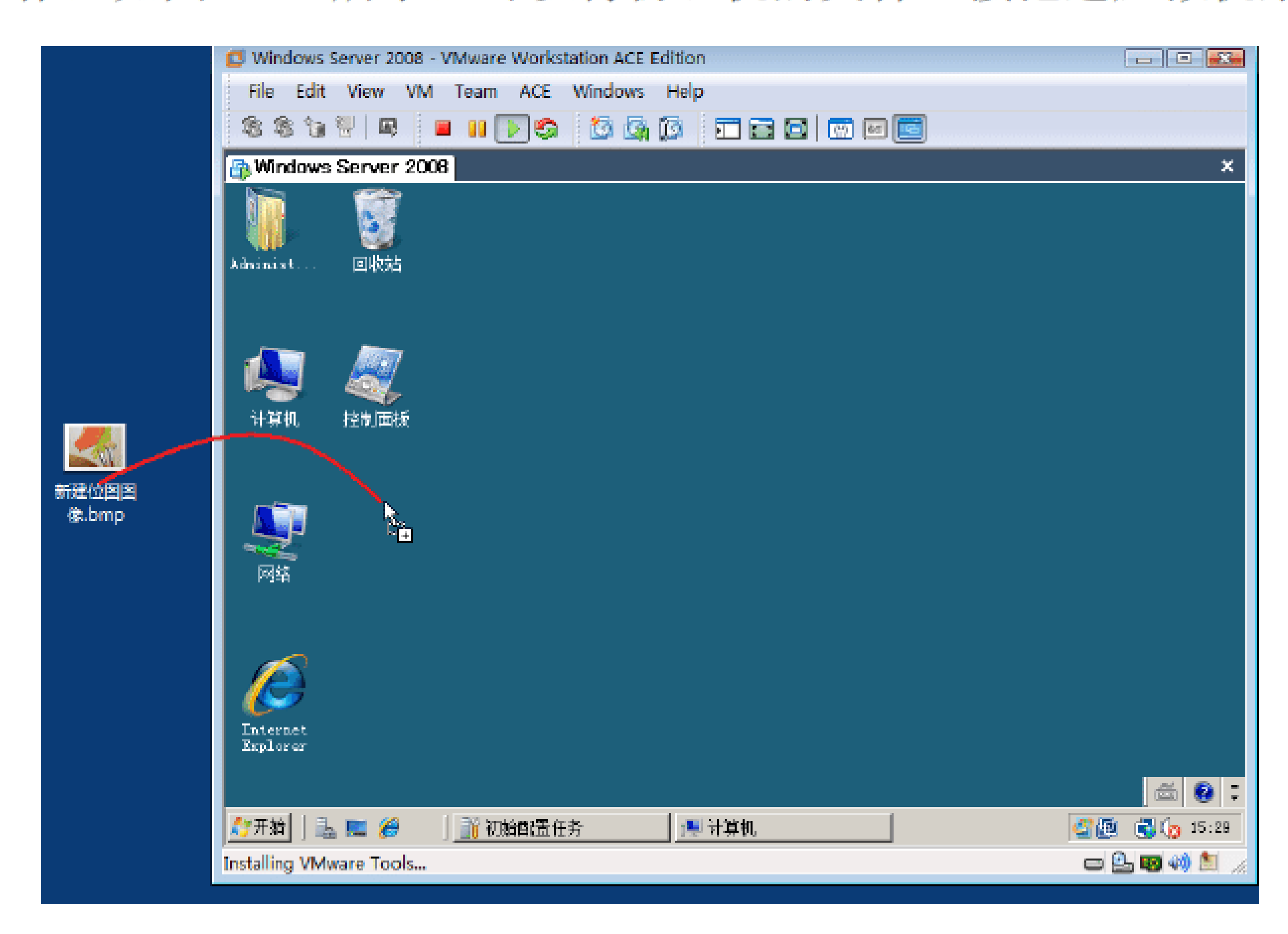


图 2-43　物理机和虚拟机之间能够拖曳复制文件

2.6.2　任务 2：更改计算机的硬件设置

在测试环境中，可能需要虚拟计算机有多个网卡，调整虚拟机的内存，给虚拟机添加多个硬盘等操作。下面的操作将会更改虚拟机的硬件。

①　单击■按钮，关闭计算机。



提示：只有关闭计算机才能添加/删除硬件。

②　如图 2-44 所示，双击 Memory 选项，可以调整内存大小。

③　如图 2-45 所示，单击 Edit VirtualMachine settings，在出现的 Virtual Machine Settings 对话框中，单击 Add 按钮，在出现的 Hardware Type 对话框中，选择 Hard Disk 选项，单击 Next 按钮。

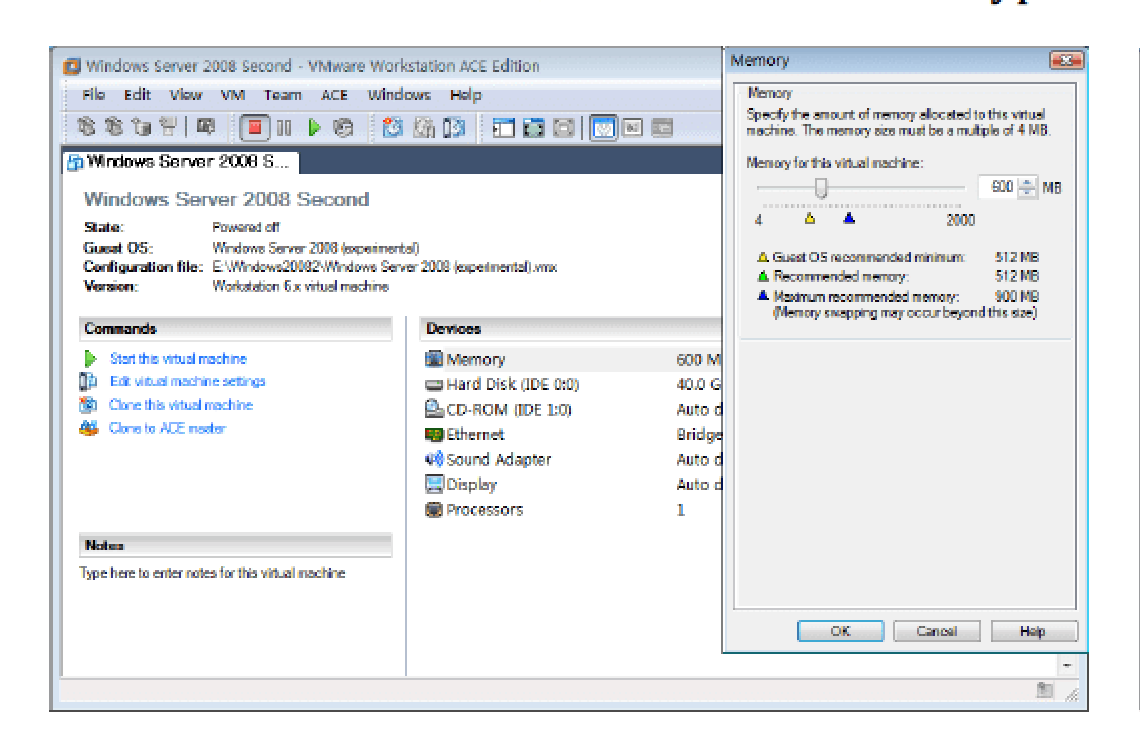


图 2-44　调整内存大小

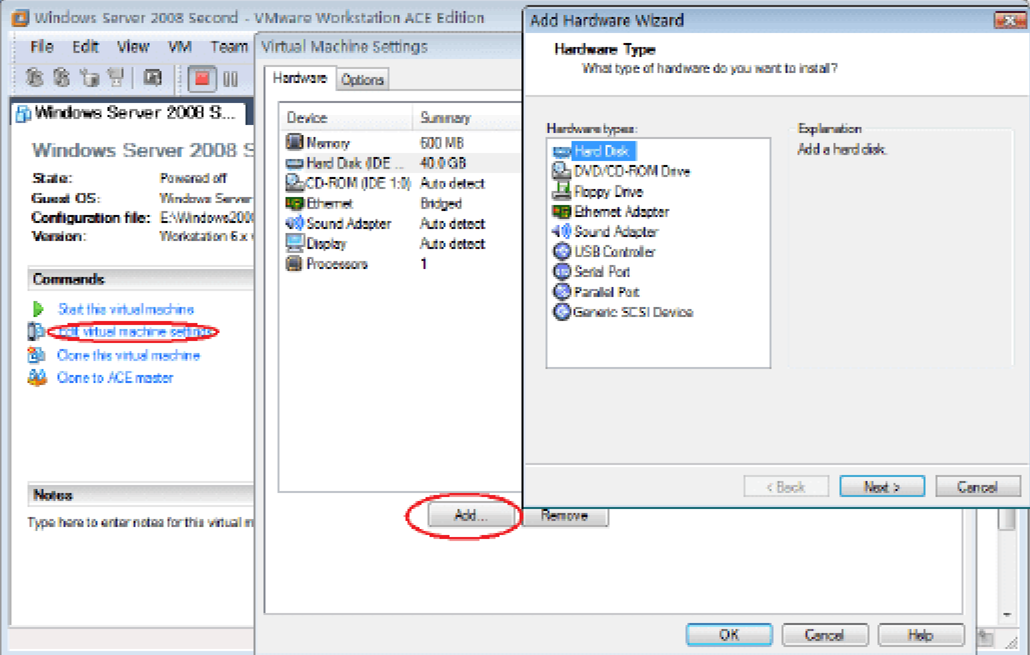
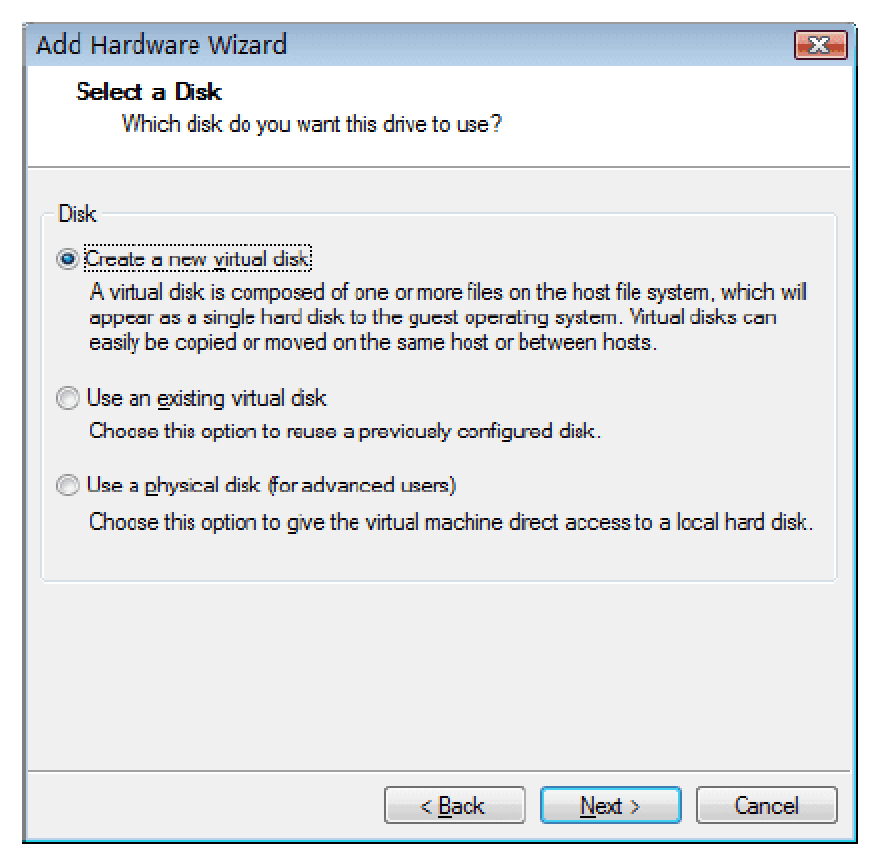


图 2-45　添加磁盘

④　如图 2-46 所示，在出现的 Select a Disk 界面中，选中 Create a new virtual disk 单选按钮。

⑤　如图 2-47 所示，在出现的 Select a Disk Type 界面中，选中 IDE 单选按钮，单击 Next 按钮。



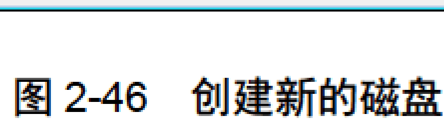


图 2-46　创建新的磁盘

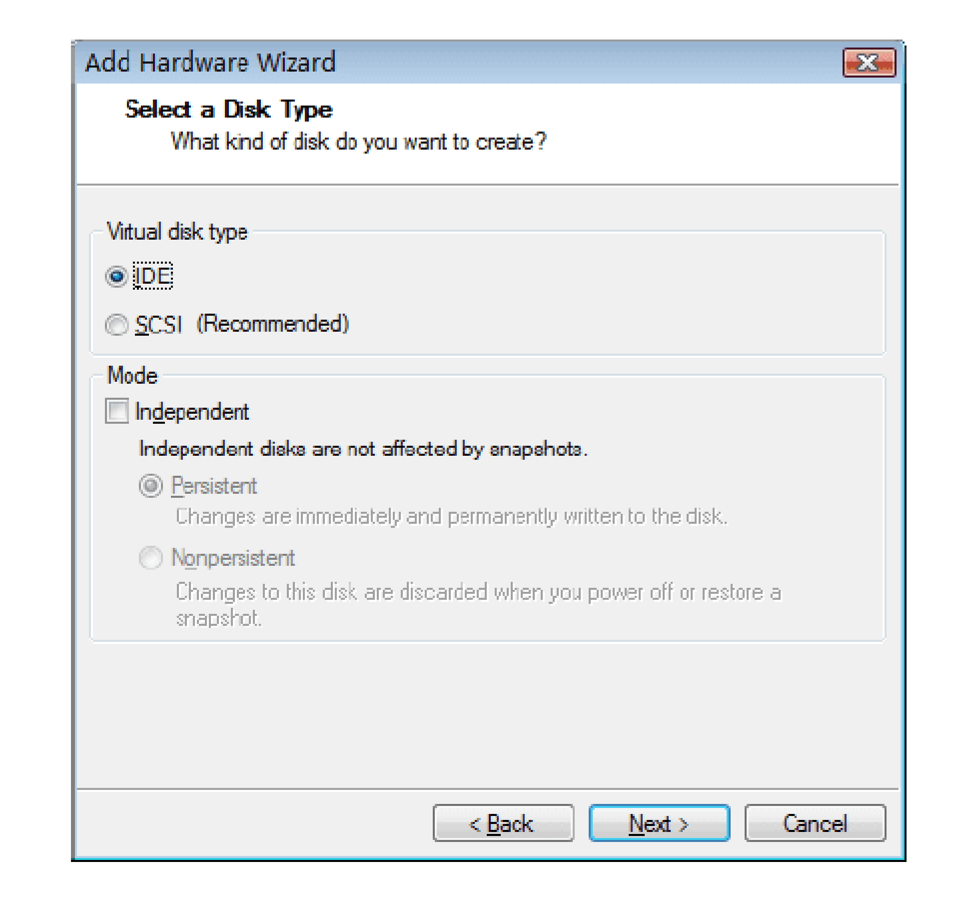


图 2-47　选择磁盘类型



提示：IDE、SATA 是普通计算机使用的硬盘，目前 SATA2 是主流，速度比 IDE 快，IDE 几乎要淘汰了。SCIS、SAS 都是服务器或者工作站所使用的硬盘类型，SCIS 目前还是主流，有独立的控制器，对系统资源占用极少，但很贵。SAS 将会逐步取代 SCIS，目前，中高端的服务器一般都采用 SAS 硬盘，价格昂贵。关于存储设备的更深研究，可参考清华大学出版社出版的《大话存储——网络存储系统原理精解与最佳实践》。

⑥　如图 2-48 所示，指定第二块磁盘文件的名字，单击 Next 按钮。

⑦　如图 2-49 所示，指定磁盘大小，单击 Finish 按钮。

⑧　单击 Edit Virtual Machine settings，单击 Add 按钮，如图 2-50 所示，在出现的 Hardware Type 界面中，选择 Ethernet Adapter 选项，单击 Next 按钮。

⑨　如图 2-51 所示，在出现的 Network Type 界面中，选中 Bridged 单选按钮，单击 Finish 按钮。

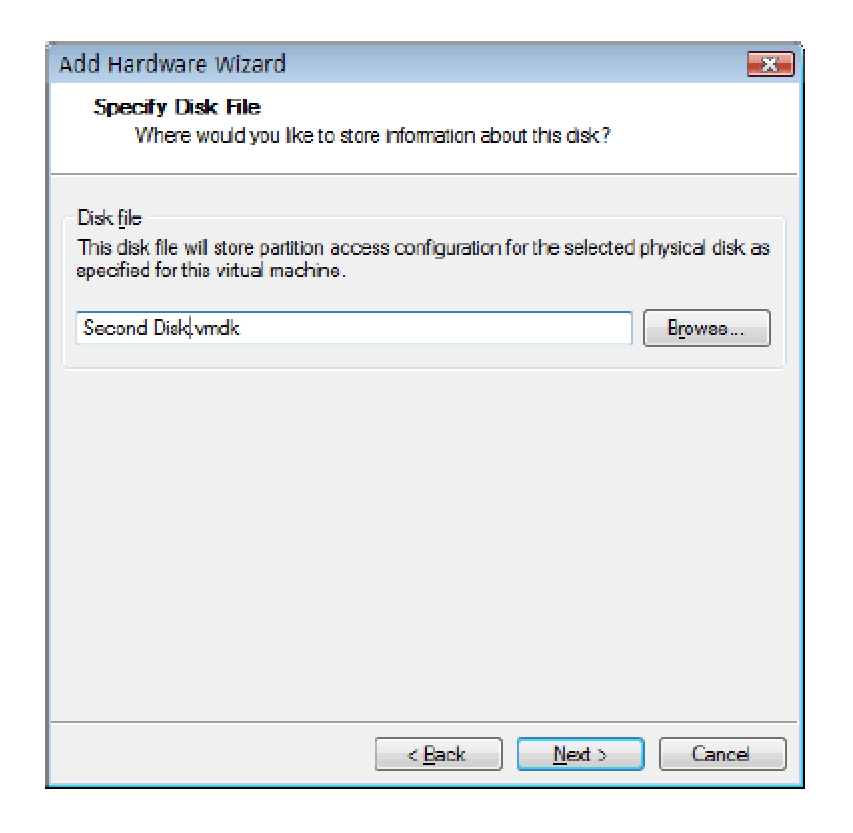


图 2-48　指定第二块磁盘文件的名字

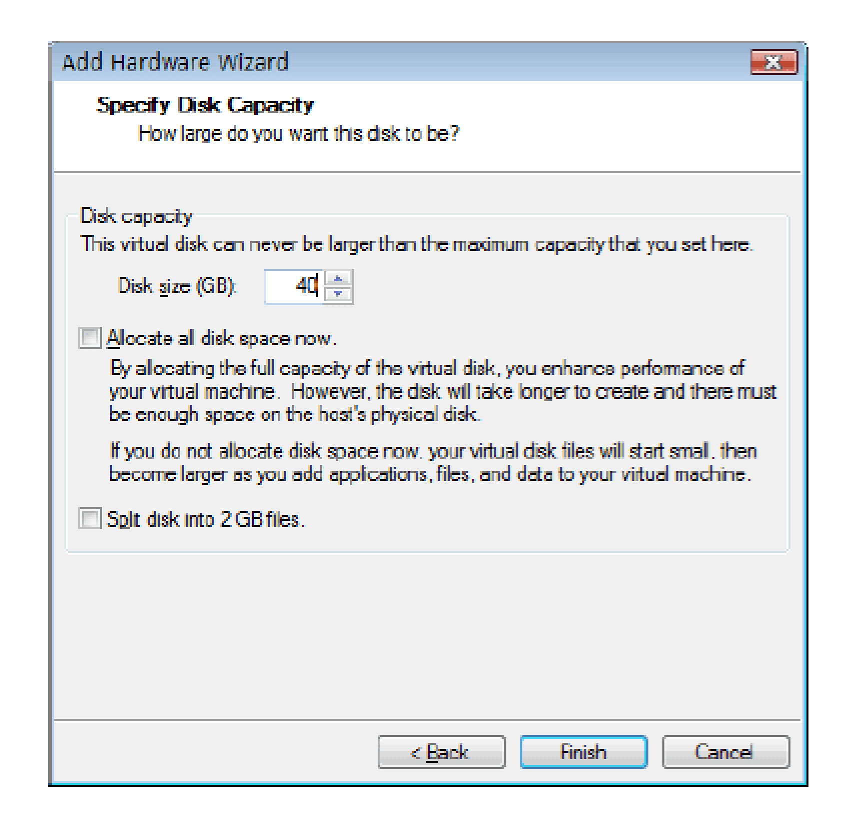


图 2-49　指定磁盘的大小

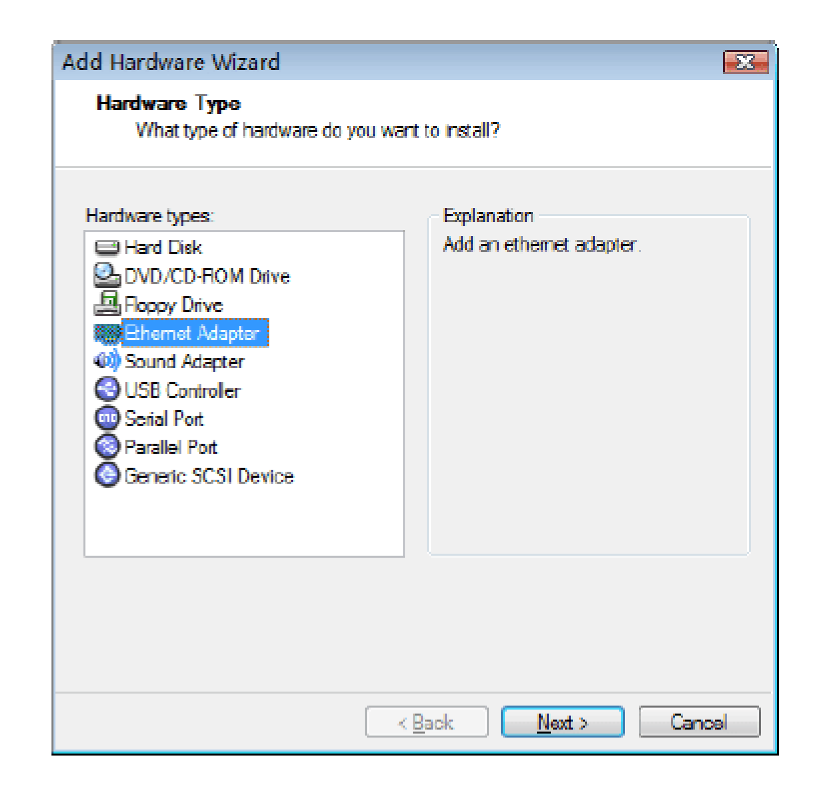


图 2-50　选择网卡

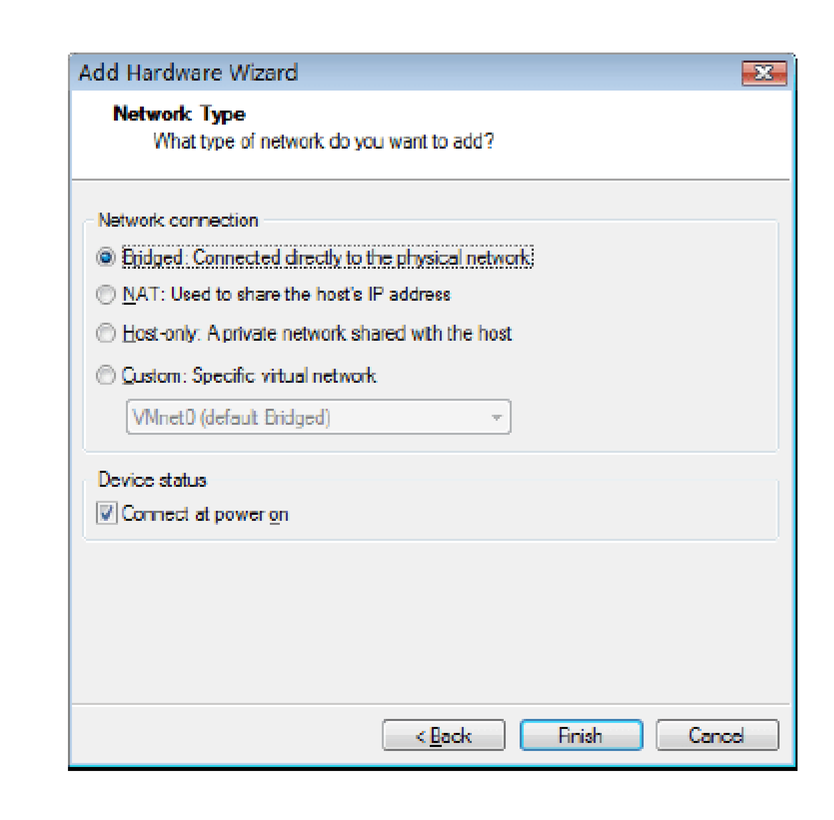


图 2-51　指定网络类型

⑩　如图 2-52 所示，单击 Edit Virtual Machine Settings，选中 floppy，单击 Remove 按钮。

⑪　如图 2-53 所示，选择 Sound Adapter 选项，单击 Remove 按钮。

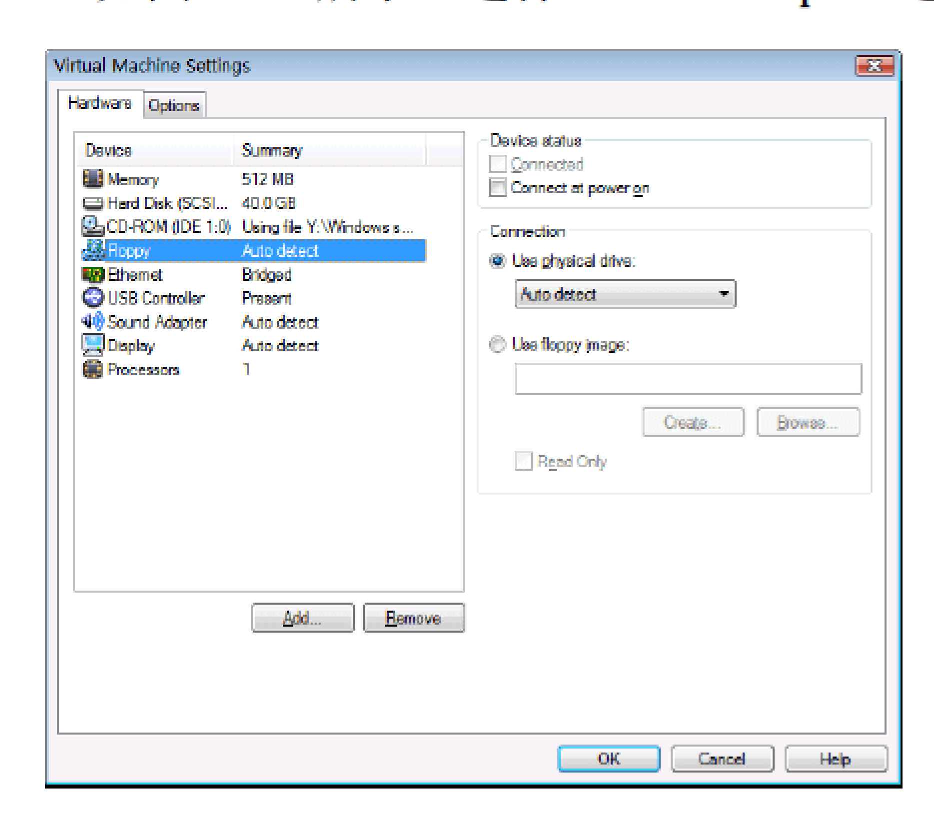


图 2-52　删除软驱

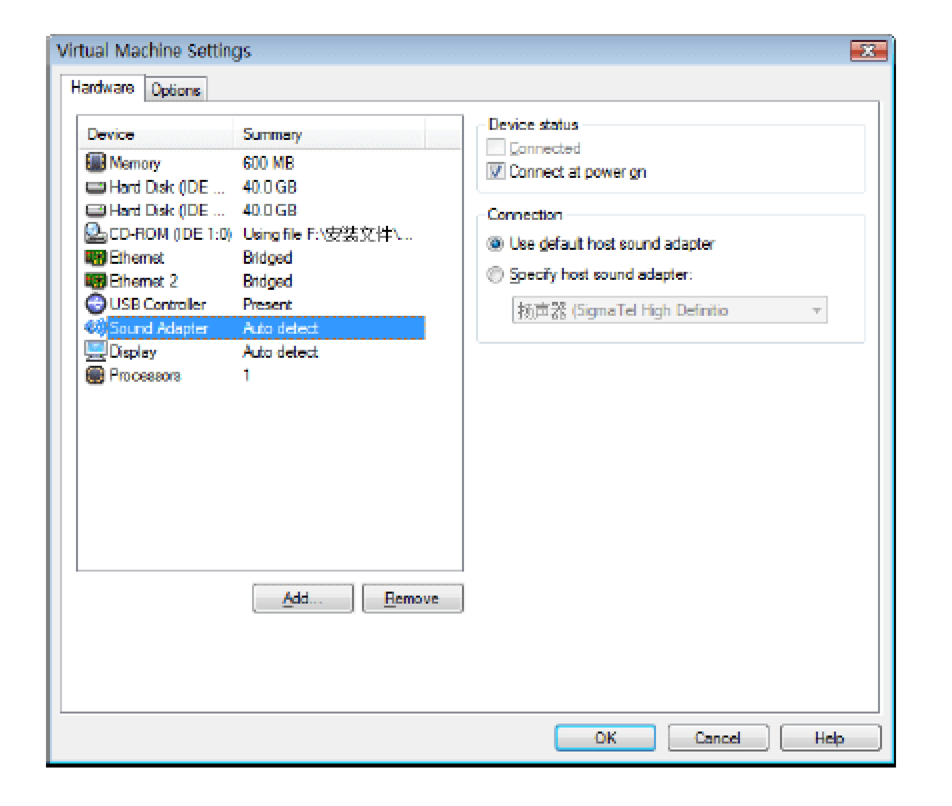


图 2-53　删除声卡

⑫　单击 按钮，启动虚拟机。按 Ctrl+Alt+Insert 组合键登录虚拟机操作系统。

⑬　登录后，单击 按钮，如图 2-54 所示，打开服务器管理器，单击“磁盘管理”选项，

能够看到新加的硬盘。经过初始化，格式化就可以使用了。

⑭ 选择“控制面板”→“网络和共享中心”命令，打开如图 2-55 所示的窗口。此时，能够看到两个连接。

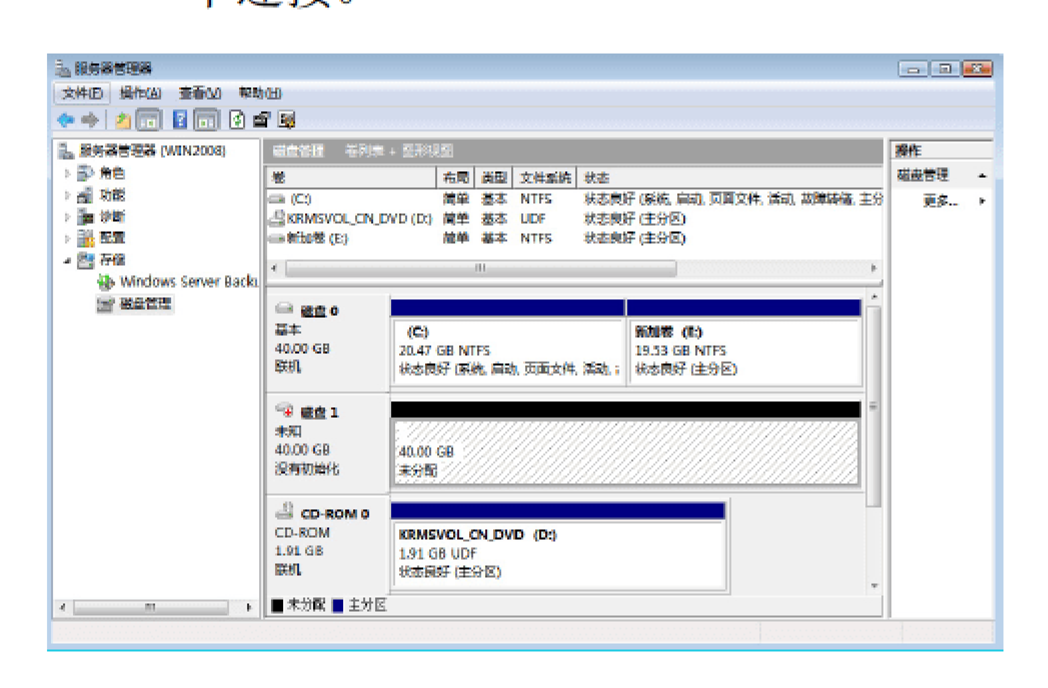


图 2-54　查看添加的磁盘

图 2-55　查看添加的网卡

⑮ 选择 VM Removable Devices 命令。

⑯ 此时，可以看到能够在虚拟系统运行的情况下更改的硬件，如图 2-56 所示，选择 Ethernet→Disconnect 命令，断开网络连接，相当于拔掉网线。



提示：可以配置 CD-ROM 使用物理光驱或使用 ISO 文件，也可以断开 CD-ROM 连接，相当于取出光盘。

⑰ 如图 2-57 所示，断开 CD-ROM 和 Ethernet 连接，双击光驱打不开，网卡显示红叉，光驱显示红叉。

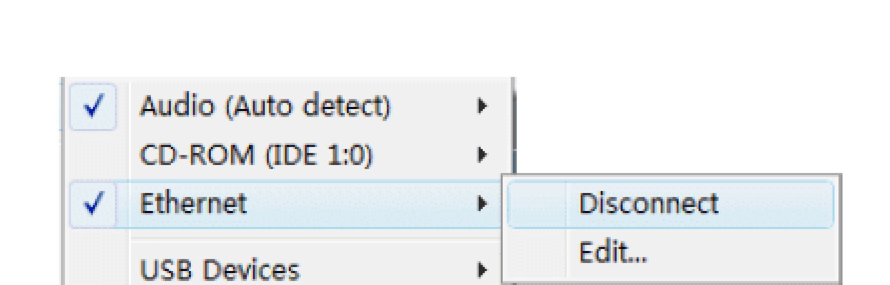


图 2-56　断开网络连接或编辑 CD-ROM

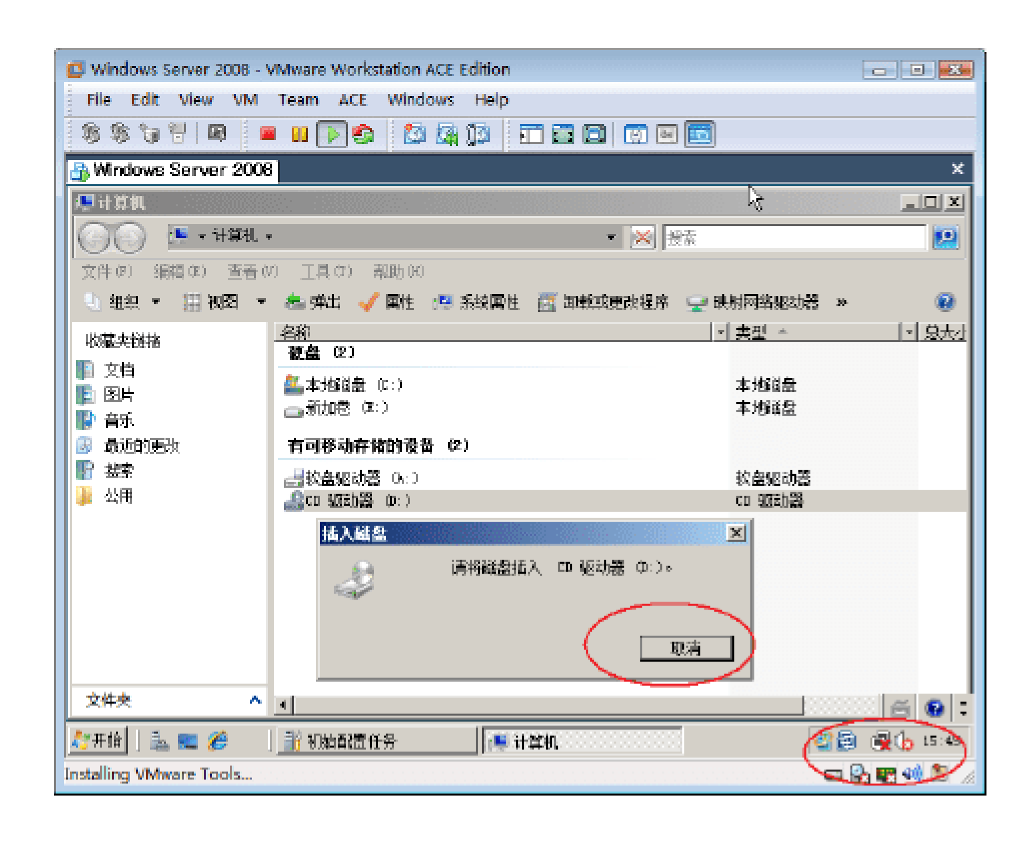


图 2-57　查看虚拟机断开的硬件

2.6.3　任务 3：为安装好的系统做快照

快照可以保存操作系统的多个状态，比如刚刚安装完操作系统后做个快照叫做 ClearSystem，后来又在虚拟操作系统中安装了 SQL Server，可以在装完 SQL Server 之后做个快照叫做 SQL Server。若现在需要一个干净的操作系统，则可以恢复到快照 ClearSystem。通过快照可以回到不同的状态。

快照是消耗磁盘空间的，没有用的快照可以删除以节省空间。

克隆系统的操作步骤如下。

① 关闭虚拟机。

② 选择 VM→Snapshot→Snapshot Manager 命令，在出现的快照管理对话框中，如图 2-58 所示，单击 Take Snapshot 按钮，输入快照名称和描述。可以做多个快照。

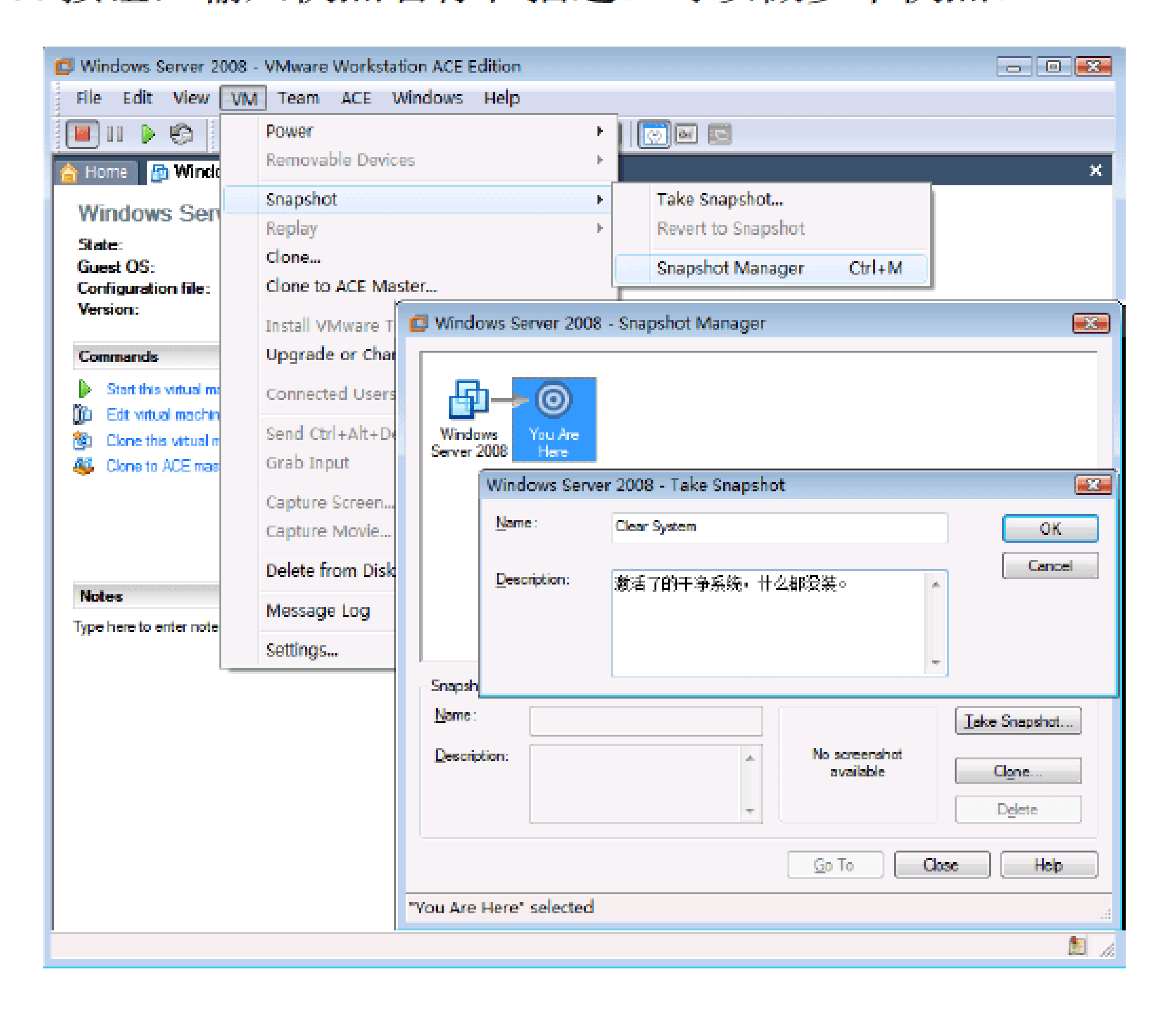


图 2-58 创建快照

③ 还原到 Clear System 状态。这是一个刚安装完系统的状态。

④ 如图 2-59 所示，打开快照管理选择 Clear System 快照，单击 Go To 按钮。

⑤ 在弹出的提示框中单击 Yes 按钮。

⑥ 再次打开快照管理。如图 2-60 所示，查看你所处的位置。

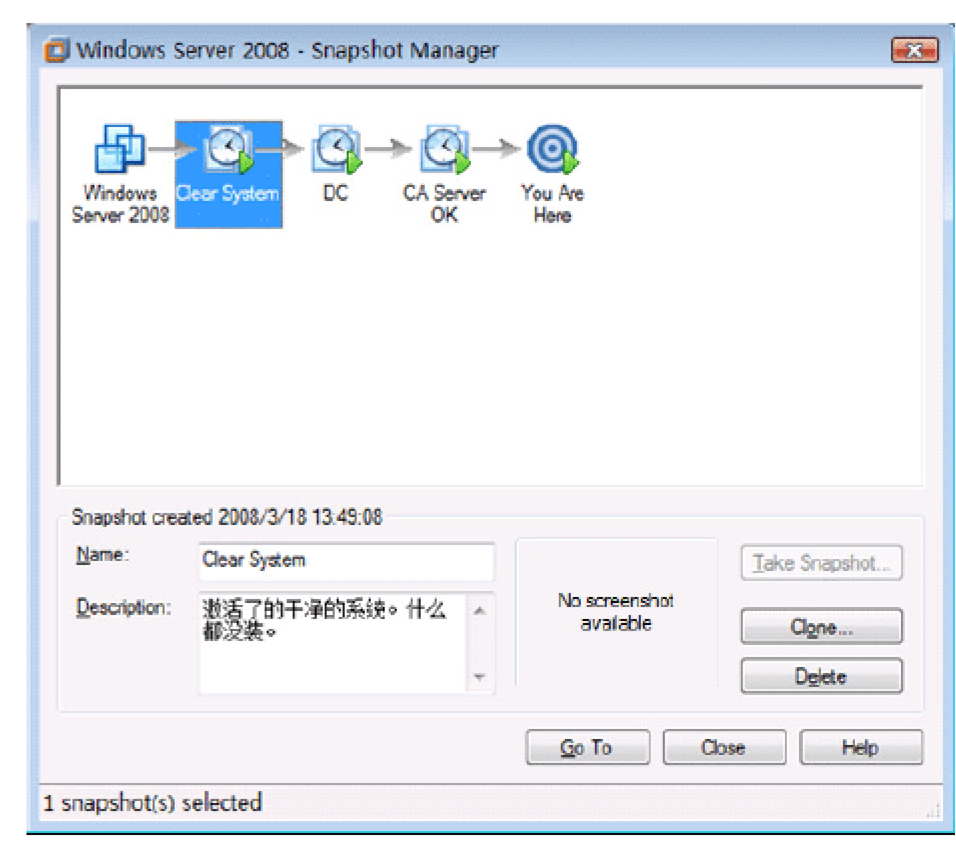


图 2-59 还原到某个快照

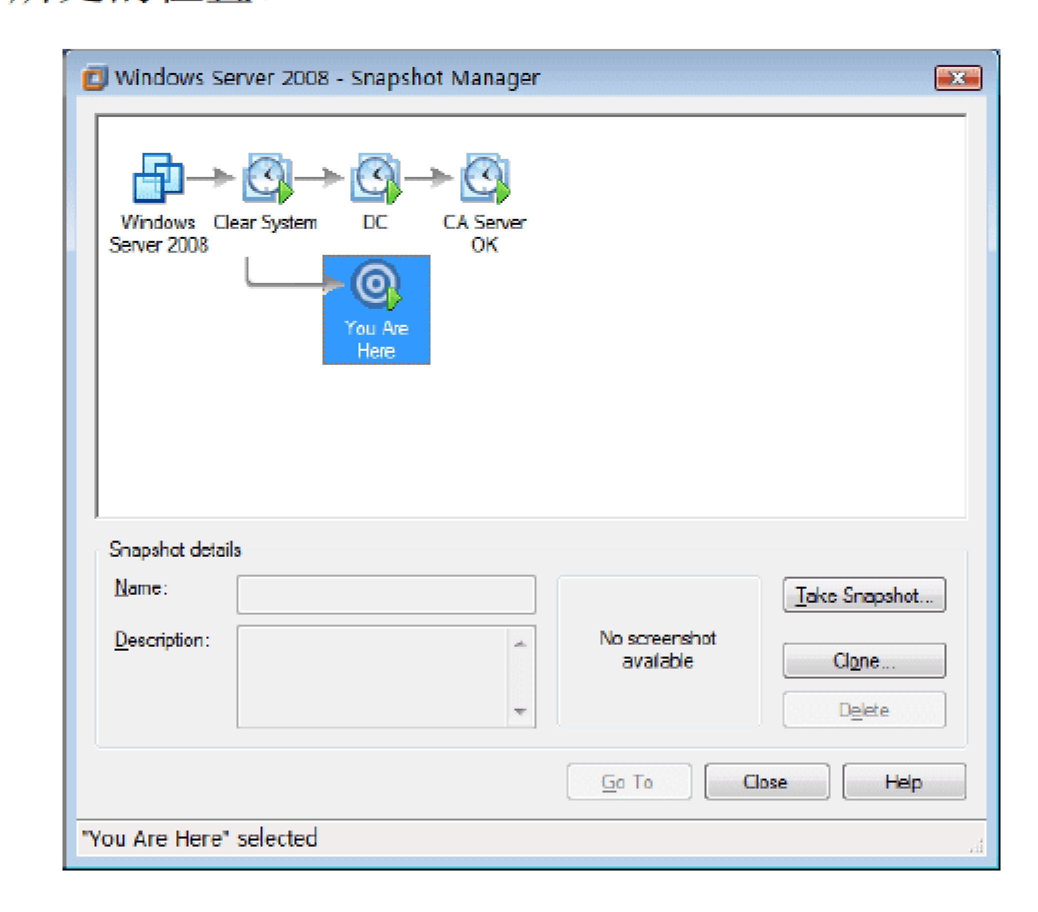


图 2-60 可以看到当前状态所处的位置

⑦ 如图 2-61 所示，选中要删除的快照，单击 Delete 按钮。

⑧ 在弹出的提示对话框中单击 Yes 按钮。如图 2-62 所示，此时可看到快照被删除了。这样就会少占用一些磁盘空间。

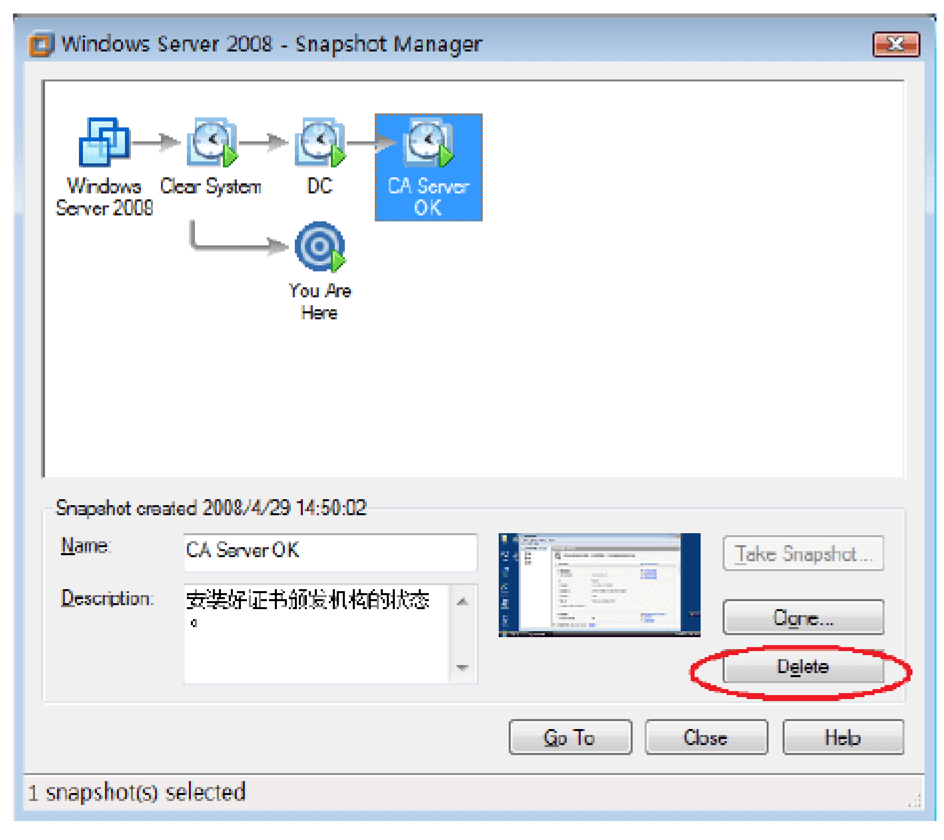
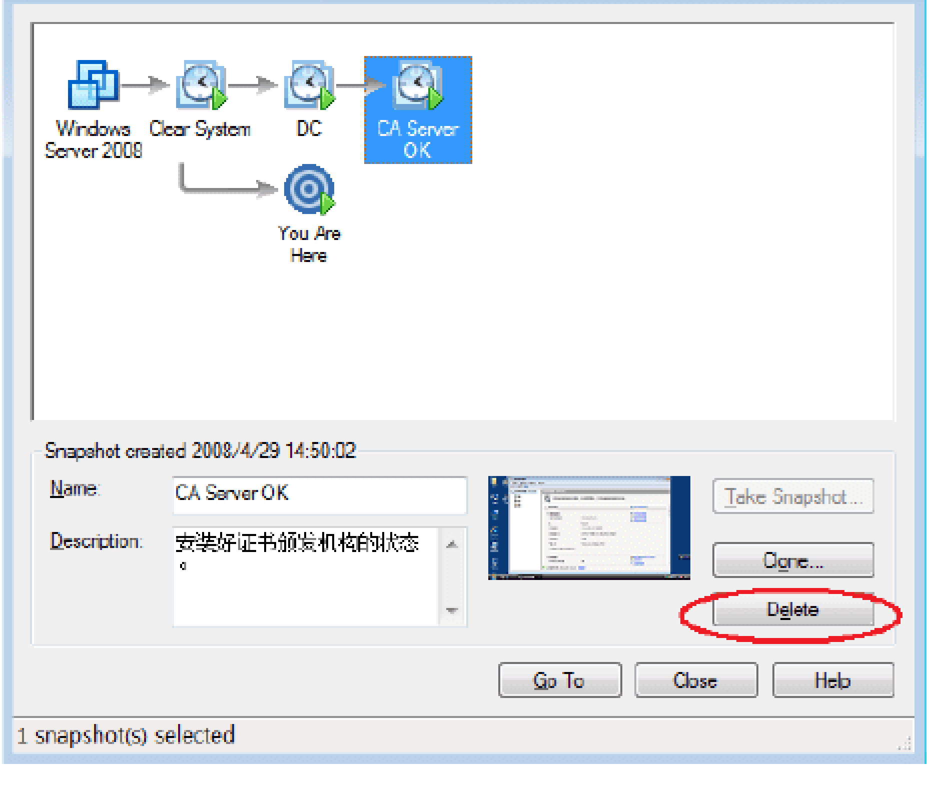



图 2-61　删除快照

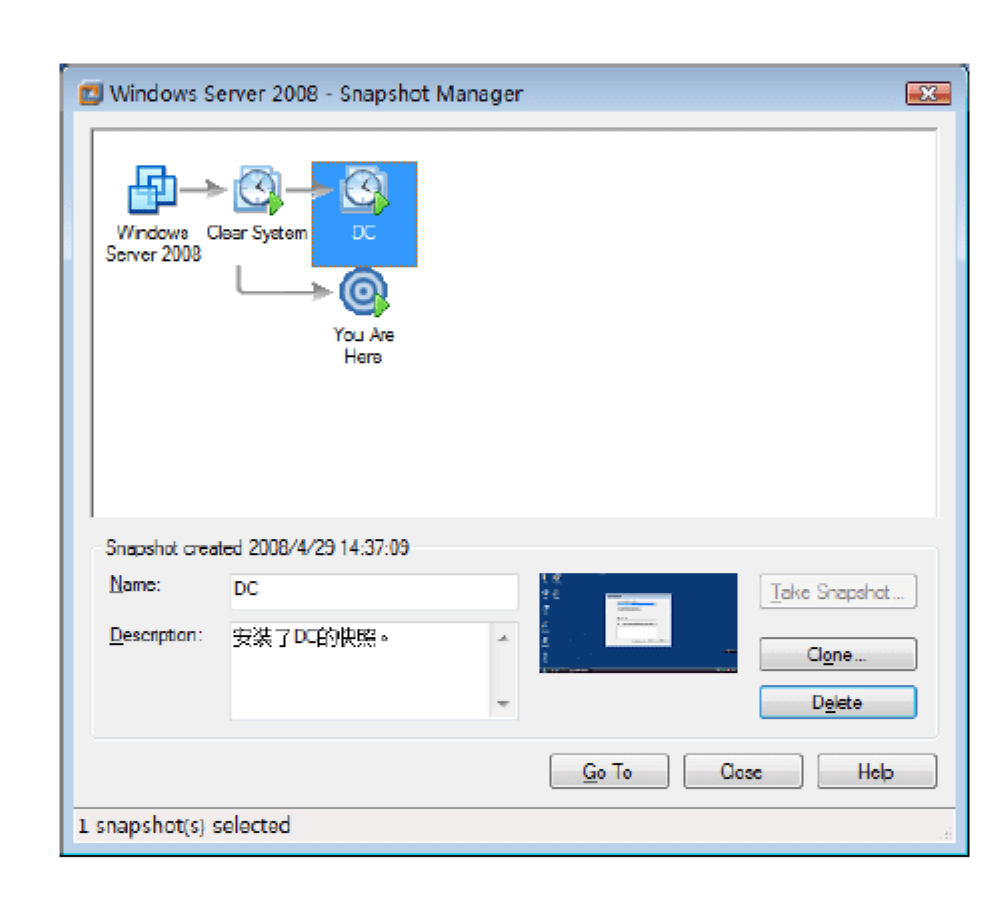


图 2-62　删除快照后

2.6.4　任务 4：克隆出多个系统

在以后的学习中，需要多个操作系统来完成实战，如果已经安装好了一个操作系统，就可以克隆出多个系统，这样可省去安装操作系统的过程。通过创建连接克隆，还可以节省磁盘空间，此时会发现新克隆出来的系统比新装的系统占用较少的空间。

可以以关闭的系统克隆出新系统，或者以关闭系统后做出的快照为基础克隆出新系统，但不能以运行着的系统做的快照克隆系统。

① 关闭虚拟机中的操作系统。

② 选择 VM→Snapshot→Snapshot Manager 命令，在出现的如图 2-63 所示的快照管理对话框中，单击 Clone 按钮后，单击“下一步”按钮。

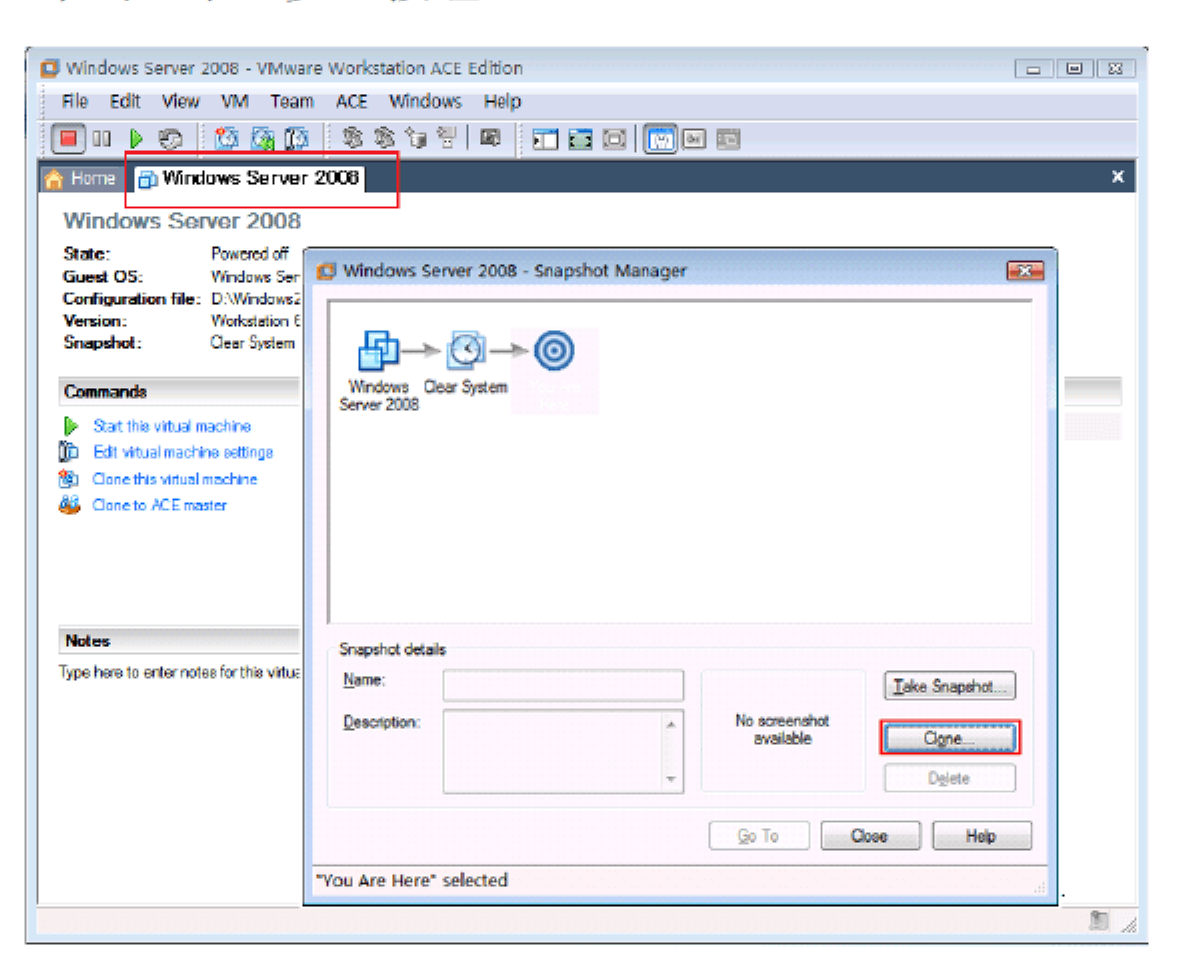


图 2-63　克隆系统

③ 如图 2-64 所示，在出现的 Clone Source 界面中，选中 An existing snapshot(powered off only)单选按钮，单击“下一步”按钮。

④ 如图 2-65 所示，选中 Create a linked clone 单选按钮，单击“下一步”按钮。

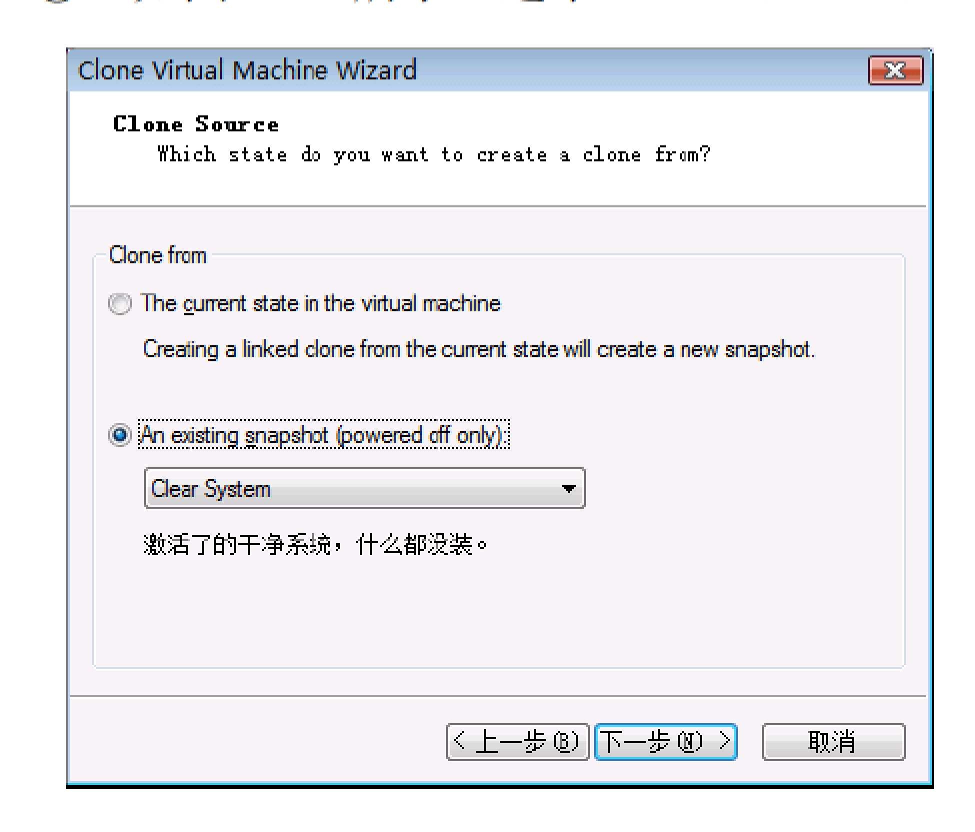



图 2-64 使用快照作为源

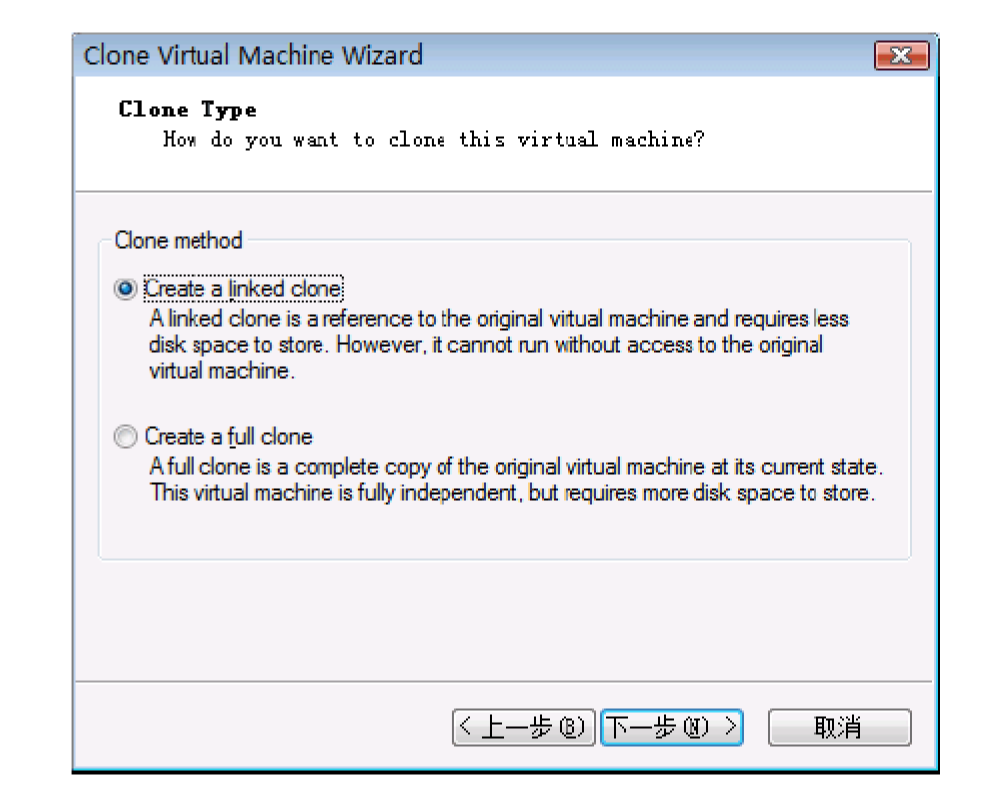


图 2-65 创建关联的克隆

注意：创建连接的克隆，可节省磁盘空间。如果原始虚拟机不能访问，则克隆出来的系统不能访问。

⑤ 如图 2-66 所示，指定虚拟机的位置和虚拟机的名称，单击“下一步”按钮，完成克隆。

⑥ 此时可在虚拟集中看到两个虚拟机操作系统，如图 2-67 所示。这两个虚拟机可以作为单独的计算机启动。


提示：但是会出现计算机名和 IP 地址冲突问题，同时计算机的 SID 也一样。SID 的全称是“安全标识符”(Security Identify)。如果想让克隆出来的新系统产生新的 SID，则需要执行下面的操作。

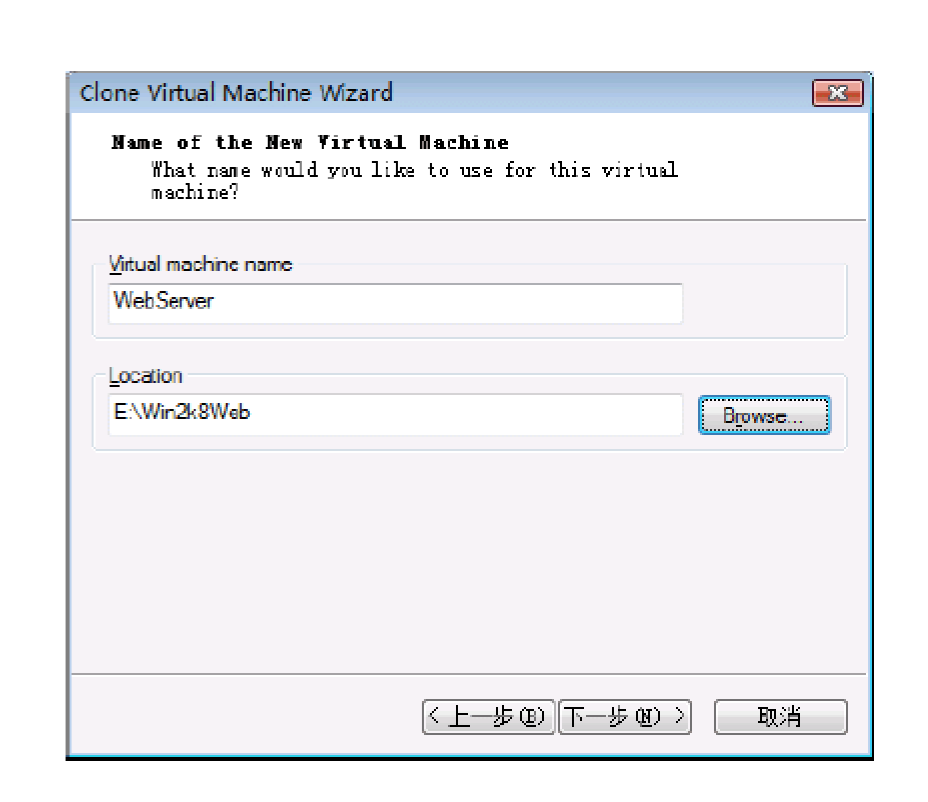


图 2-66 指定虚拟机的名称和位置

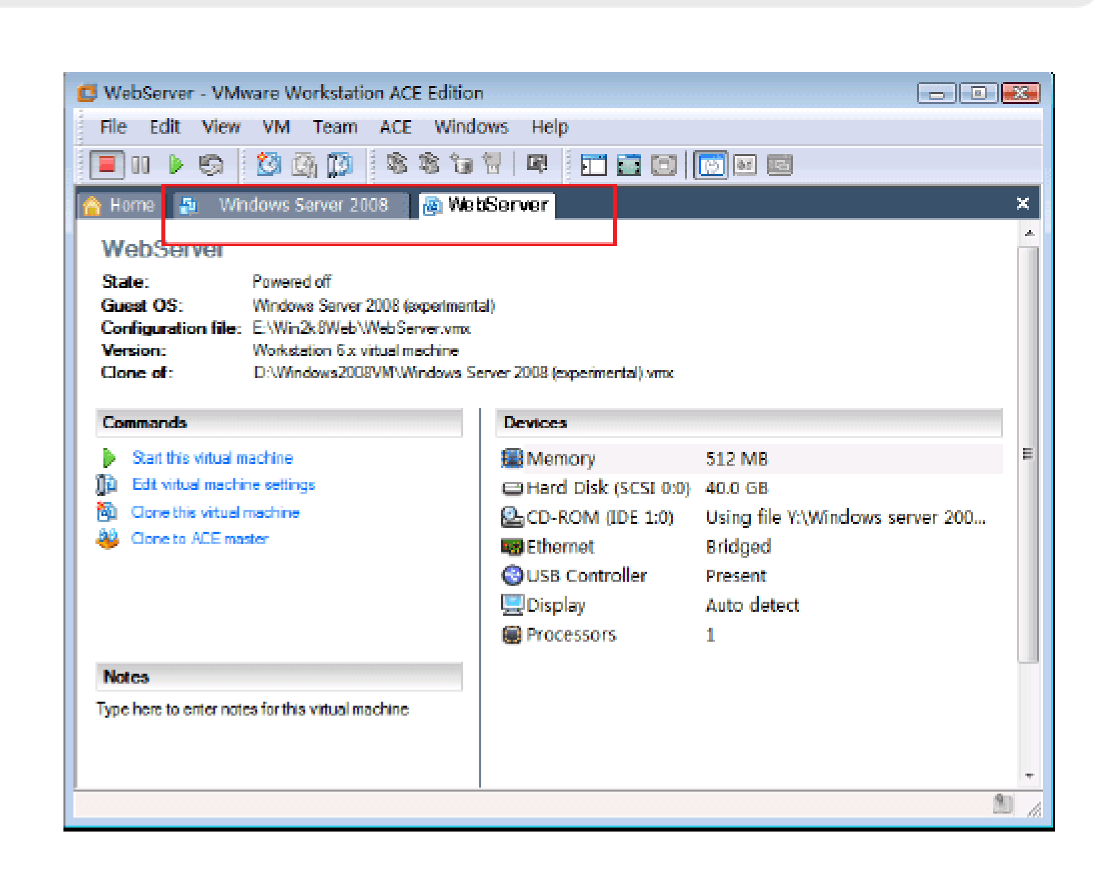


图 2-67 克隆出来的系统

⑦ 单击按钮启动克隆出来的新系统。输入管理员账户和密码登录。

⑧ 如图 2-68 所示，选择“开始”→“运行”命令，输入 sysprep，单击“确定”按钮。

⑨ 如图 2-69 所示，打开 C:\windows\system32\sysprep 目录。双击 sysprep 选项，选择如图，选中“通用”复选框，单击“确定”按钮，关机。

⑩ 单击按钮启动虚拟机操作系统。如图 2-70 所示，会出现安装时的界面。

⑪ 如图 2-71 所示，输入新的计算机名称，单击“开始”按钮。

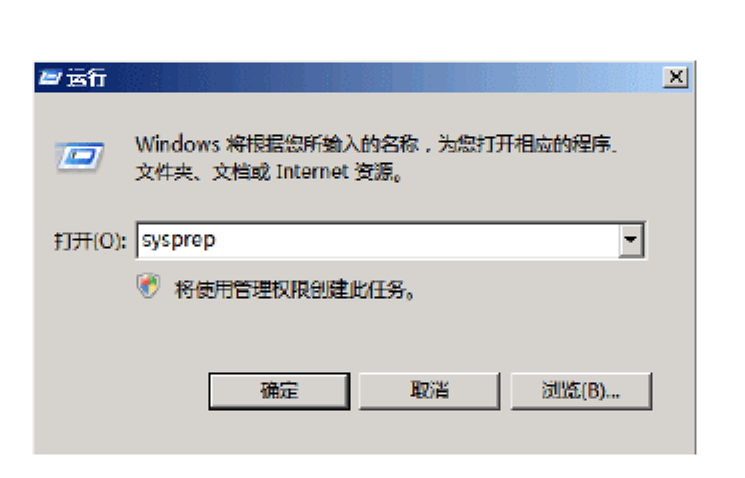


图 2-68　运行 sysprep

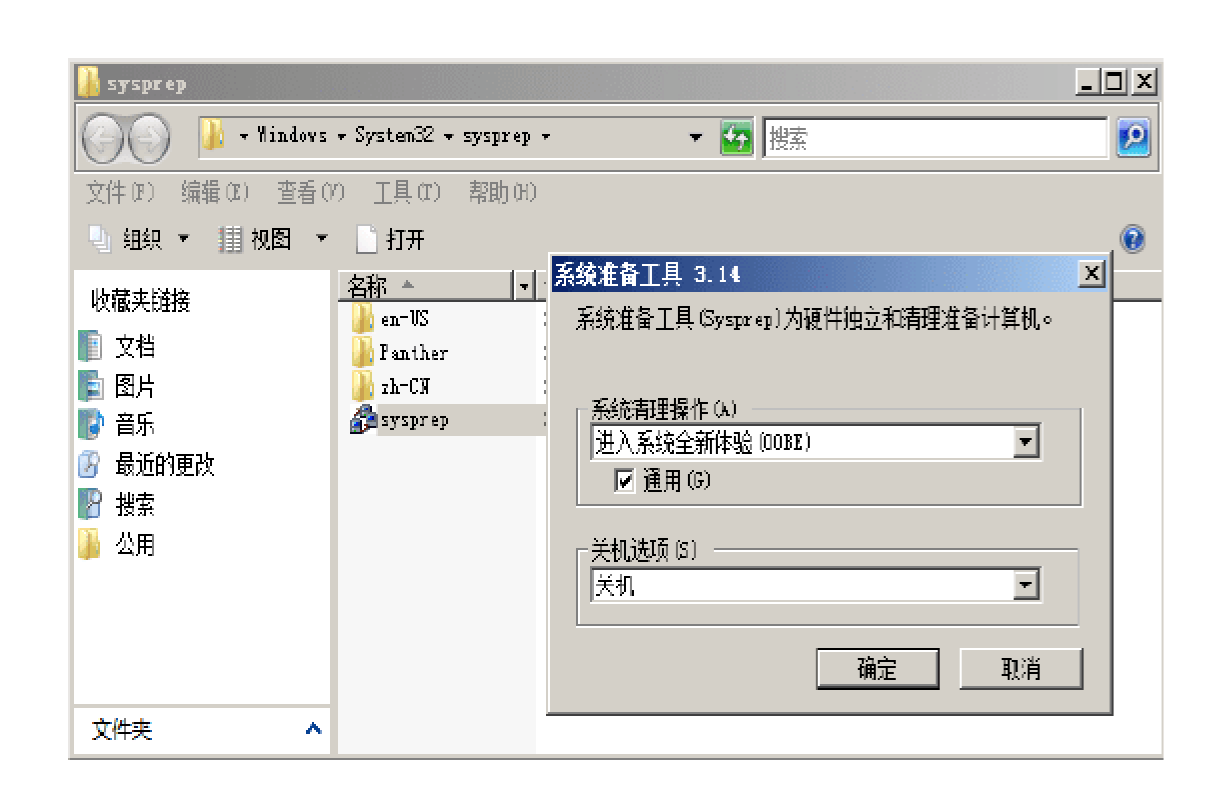


图 2-69　设置通用模式

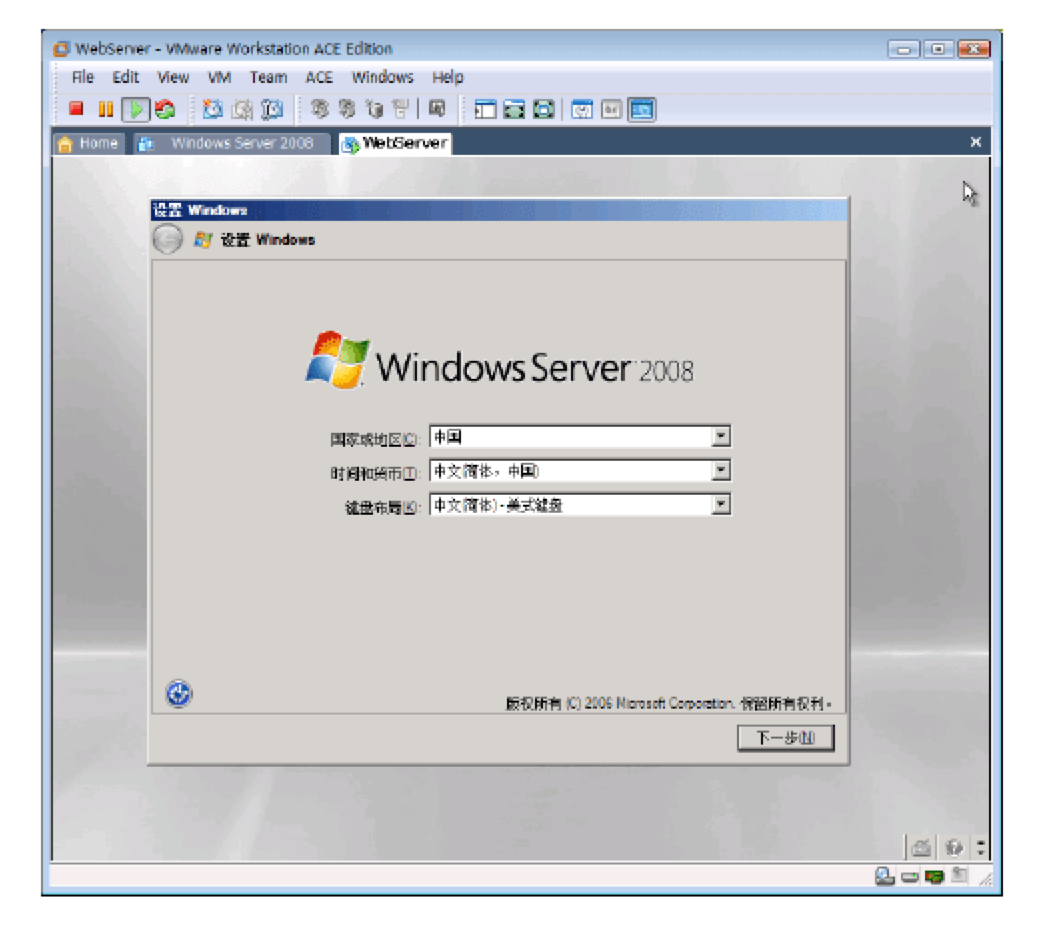


图 2-70　重新封装后启动

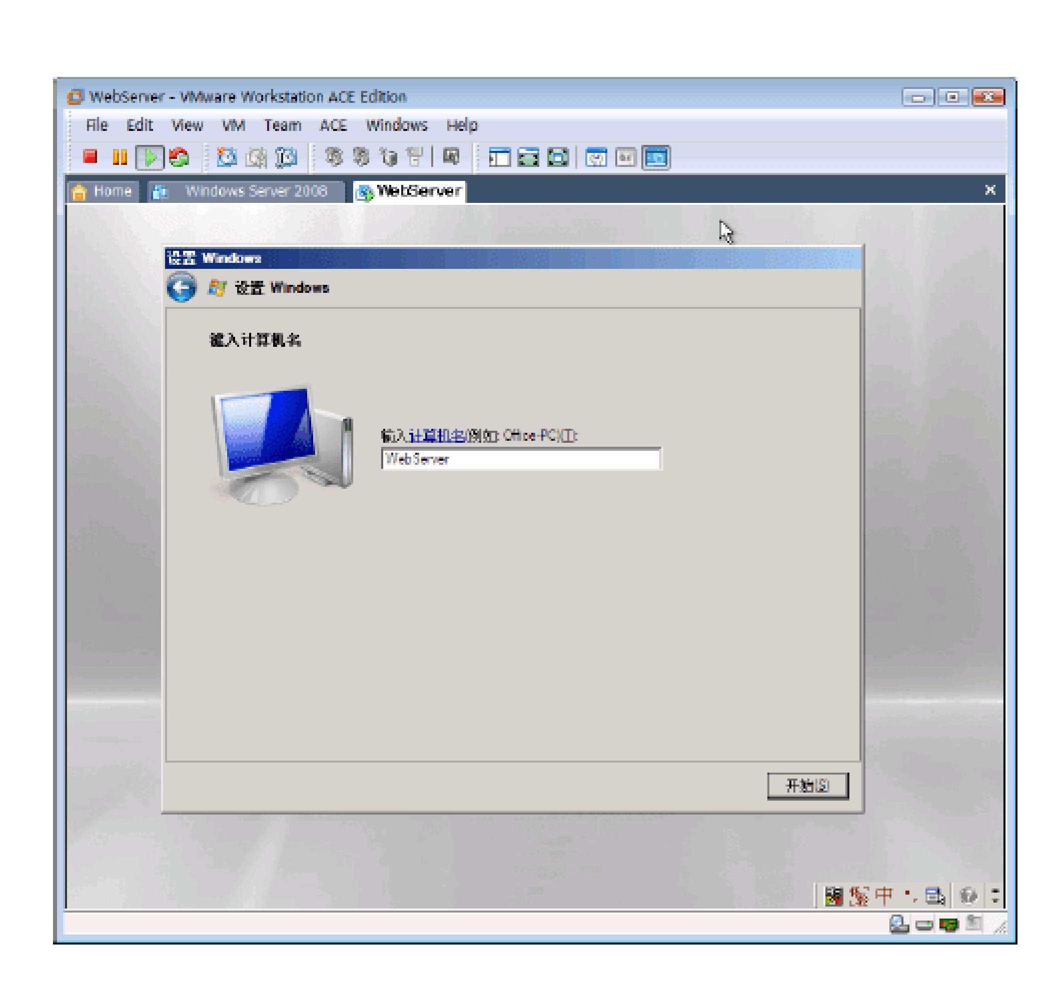


图 2-71　输入计算机名称

⑫　完成之后，进入系统要求重设管理员密码。

⑬　需要重新激活，如图 2-72 所示。

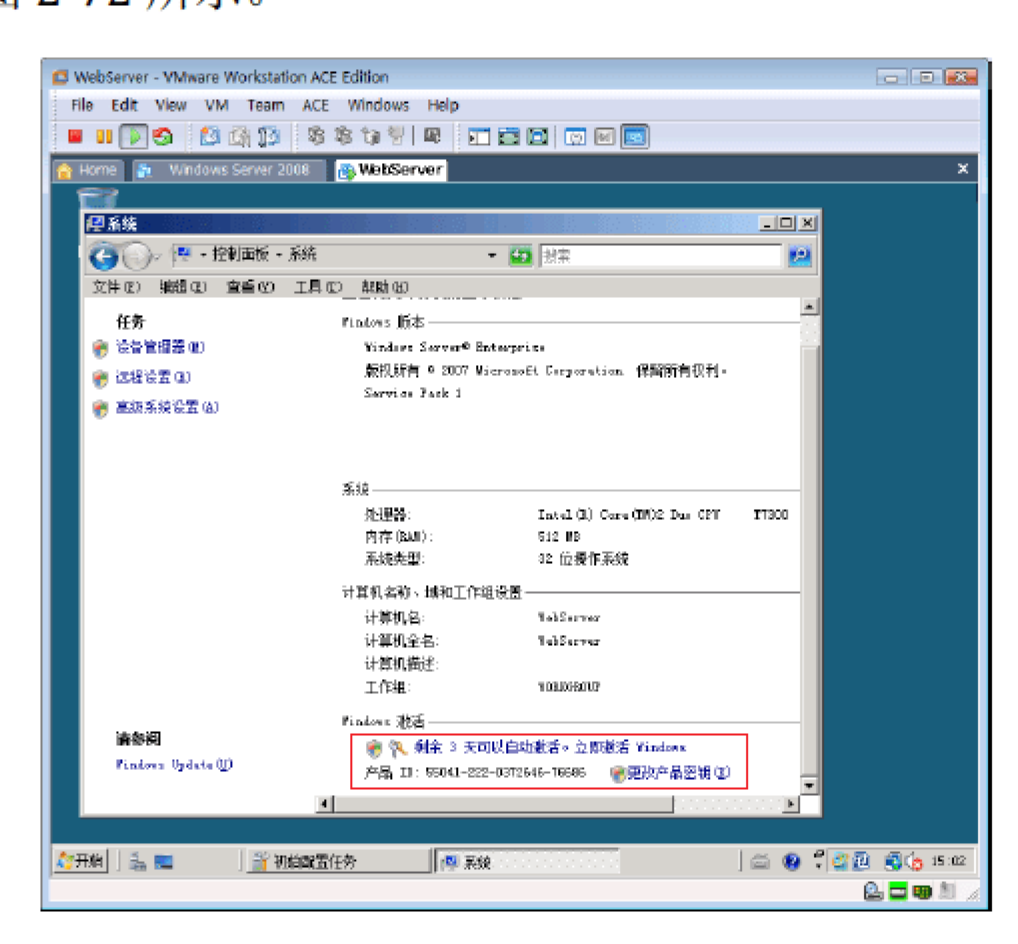


图 2-72　需要重新激活

2.7 实战：安装 Windows Server Core

Windows Server Core(服务器核心)是 Windows Server 2008 新的默认组件，没有资源管理器(Windows 外壳程序)，仅包含简单 Console 窗口和一些管理窗口，但是可以运行 MMC，可以用作域控制器 活动目录 Active Directory、DNS 域名解析服务器、FTP 文件服务器、Print 打印服务器、Streaming Media 流媒体服务器或 Web 服务器等。它的特点是高效、占用内存小，相对安全高效，类似没有安装 x-Window 的 Linux。不推荐普通用户使用。

Server Core 安装为用户提供了以下优势。

- 减少维护：因为在 Server Core 版本中用户只是安装了必不可少的 DHCP、文件、DNS 以及活动目录这些基本的服务器角色，这样就比安装完整的 Longhorn Server 减少了维护系统所需的时间和精力。
- 减少攻击面：由于 Server Core 进行的是最小的安装动作，所以就保证了更少的应用程序运行在服务器上，这样无形中就减少了服务器受攻击的可能。
- 减轻管理： 因为更少的应用程序和服务被安装在基于 Server Core 的服务器上，就使得管理方面的开销也大大降低。
- 降低硬件需求： Server Core 的安装只需大约 800 MB 的硬盘空间，快速安装则不到 500 MB。

任务描述

安装 Windows Server 2008 企业版核心，并能够完成常规配置，在命令行状态下完成计算机名称更改，IP 地址更改，计算机激活。

实战环境

- VMware 6.02 软件
- Windows Server 2008 安装光盘的 IOS 文件
- 能够连接到 Internet

实战目标

- 安装 Windows Server 2008 企业版核心
- 显示 Server Core 可用的命令
- 在命令行界面下更改计算机名
- 在命令行界面下更改网络连接设置
- 在命令行界面下激活服务器
- 启用远程桌面
- 启用 Windows 防火墙

2.7.1 任务 1：安装 Windows Server 2008 企业版核心

① 双击桌面上的图标，选择 File→New→Virtual Machine 命令。

② 在向导中单击“下一步”按钮，选中 Typical 复选框。

③ 选中 Microsoft Windows，Version 选择 Windows Server 2008，单击“下一步”按钮，输入虚拟

的名字，并确定存储位置(最少有 6 GB 大小)。

④ 在网络类型中，选择 Use bridged networking。

⑤ 指定磁盘大小 40 GB。

⑥ 单击“下一步”按钮，单击“完成”按钮。

⑦ 双击 CD-ROM (IDE 1:0)，单击 Browse 按钮，找到 Windows Server 2008 的安装盘。单击 OK 按钮。

⑧ 单击▷按钮，开启虚拟机。单击“下一步”按钮。

⑨ 单击“现在安装”按钮。如图 2-73 所示，选择 Windows Server 2008 Enterprise(服务器核心安装)选项，单击“下一步”按钮。

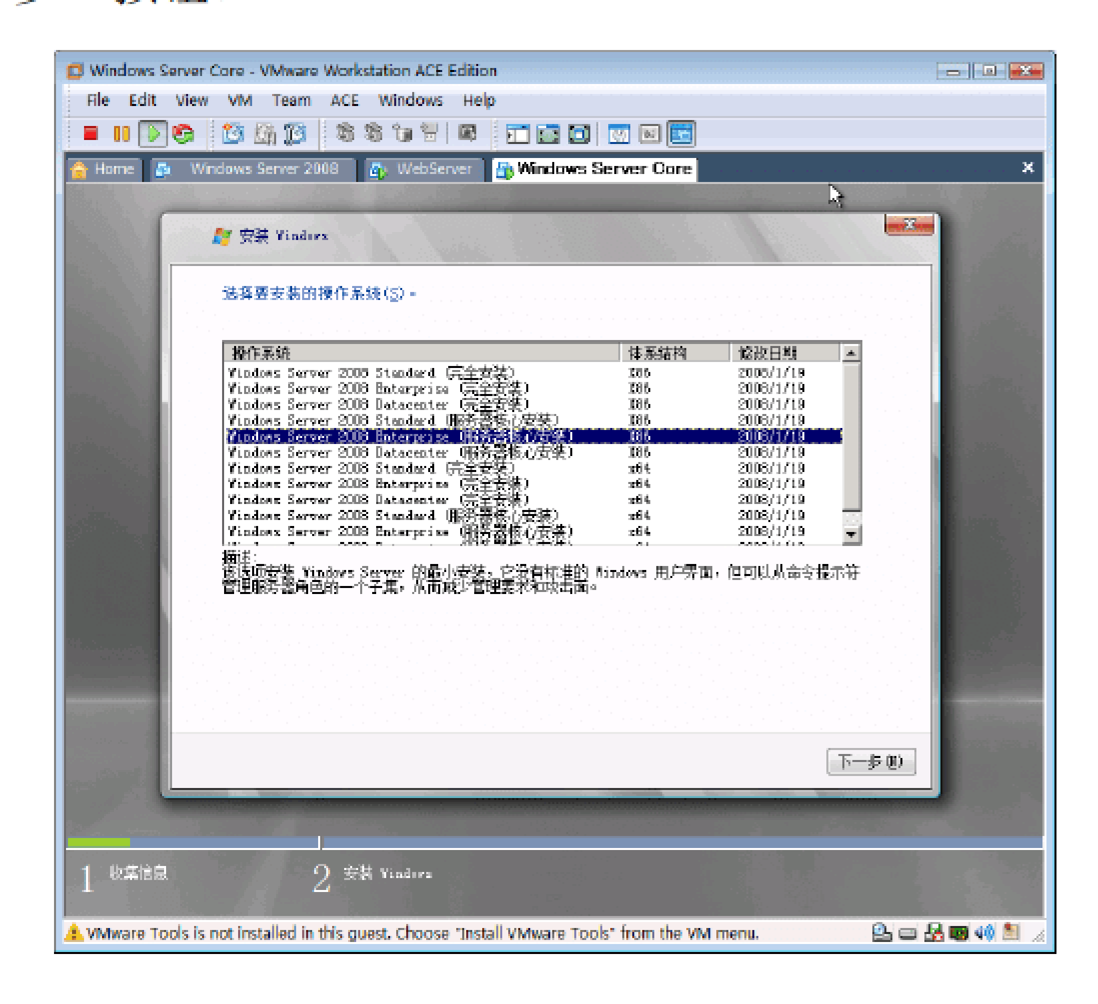


图 2-73　选择 Windows Server Core 企业版

⑩ 选中“我接受许可条款”单选按钮，单击“下一步”按钮。

⑪ 选择“自定义(高级)”选项，选择“驱动器选项(高级)”选项。

⑫ 单击“新建”按钮。

⑬ 指定磁盘大小 20000 MB，单击“应用”按钮。

⑭ 选中刚创建的分区，单击“下一步”按钮。

⑮ 重启系统，按 Ctrl+Alt+Insert 组合键登录系统。

⑯ 单击“其他用户”按钮。

⑰ 输入用户名 administrator，密码为空，如图 2-74 所示。单击➡按钮，在弹出的提示框中单击“确定”按钮，如图 2-75 所示。

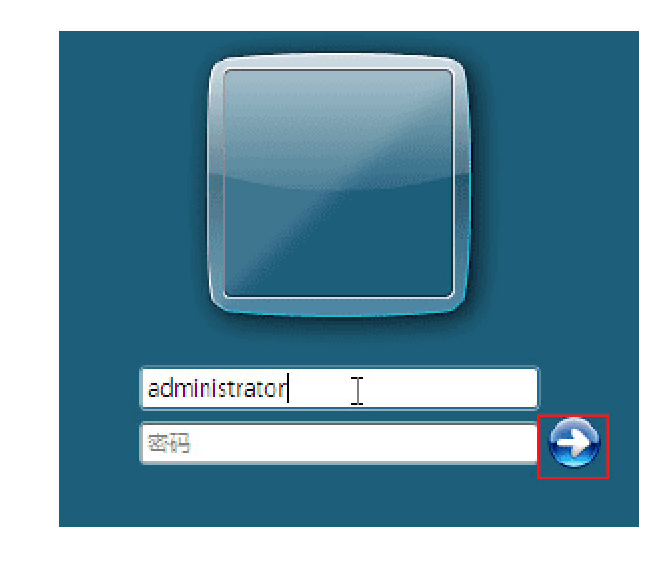
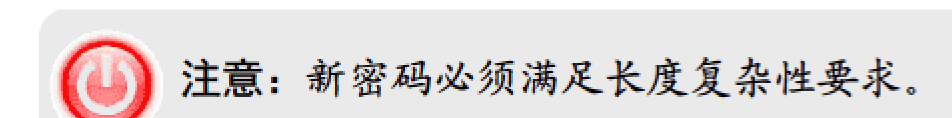


图 2-74　输入管理员账户，密码为空



图 2-75　需要更新密码

⑱ 如图 2-76 所示，输入新密码。单击 按钮，登录后即可看到一个命令行界面，如图 2-77 所示。



注意：新密码必须满足长度复杂性要求。

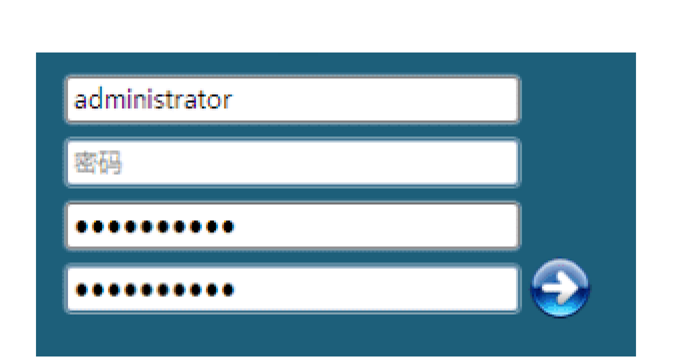


图 2-76 输入新密码

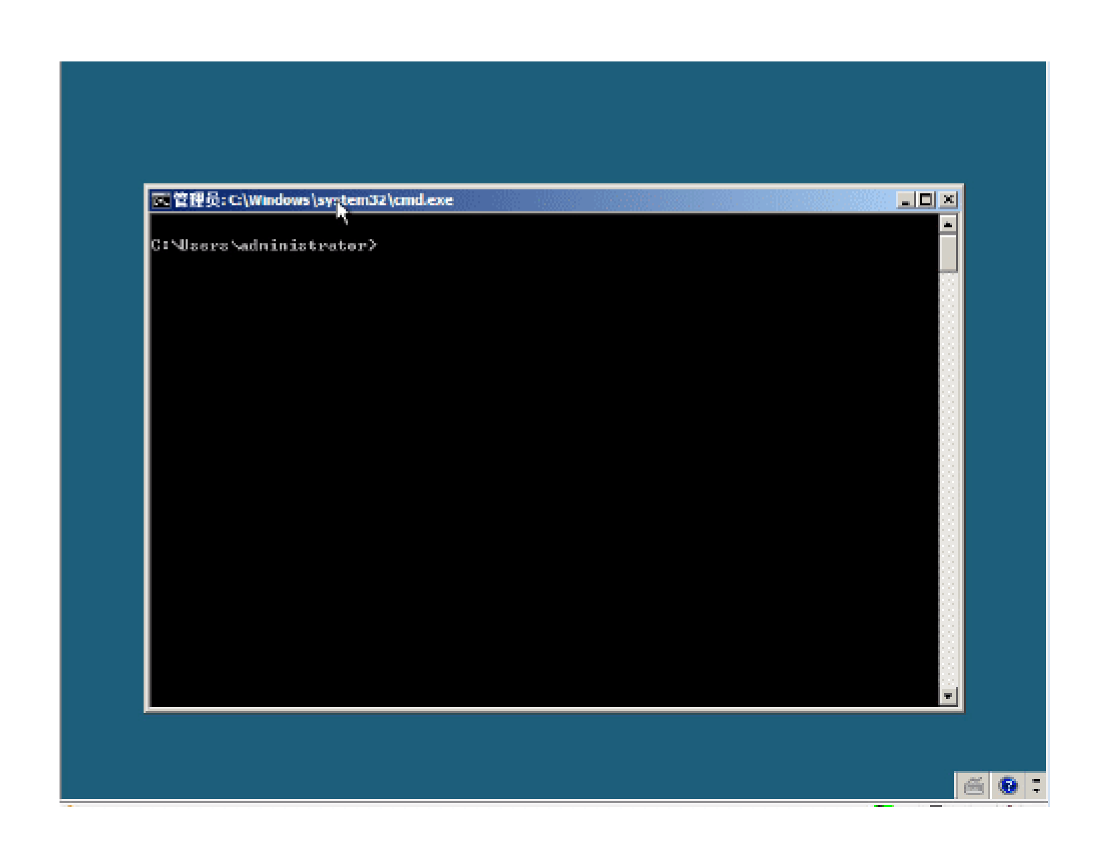


图 2-77 登录后的界面

2.7.2 任务 2：显示 Server Core 可用的命令

① 以管理员的身份登录 Windows Server 核心服务器。

② 输入：cd \。

③ 在 C 盘根目录下，输入：cd Windows\system32。

④ 如图 2-78 所示，在 C:\Windows\system32 目录下，输入：cscript scregedit.wsf /cli 将会列出 Server Core 中提供的一个常用的命令行汇总。

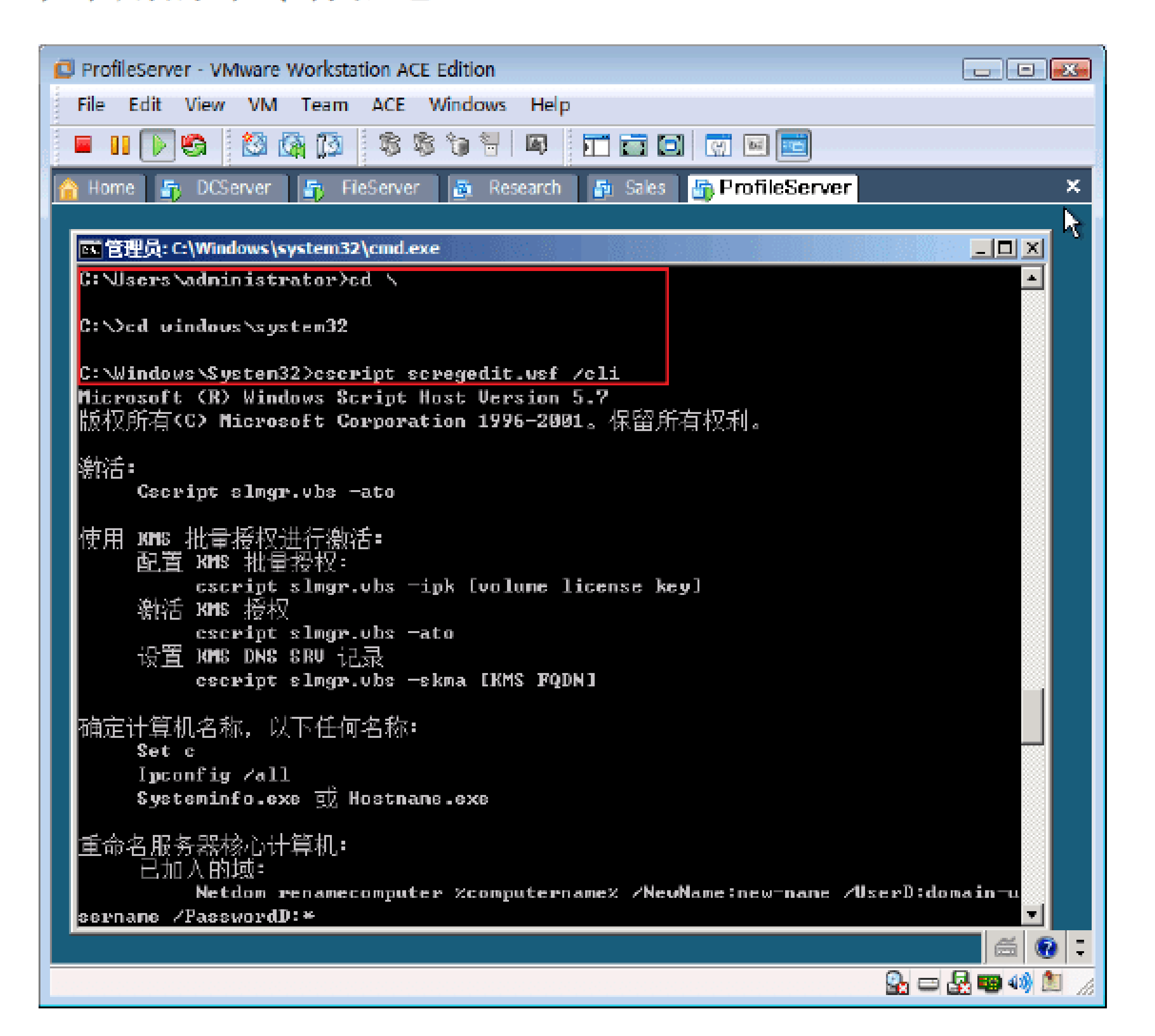


图 2-78 显示常用的命令

Server Core 中常用命令汇总如下。

- 激活

```
Cscript slmgr.vbs -ato
```

- 使用 KMS 批量授权进行激活
- 配置 KMS 批量授权

```
cscript slmgr.vbs -ipk [volume license key]
```

- 激活 KMS 授权

```
cscript slmgr.vbs -ato
```

- 设置 KMS DNS SRV 记录

```
cscript slmgr.vbs -skma [KMS FQDN]
```

- 确定计算机名称

```
Set c
Ipconfig /all
Systeminfo.exe 或 Hostname.exe
```

- 重命名服务器核心计算机
- 已加入的域

```
Netdom renamecomputer %computername% /NewName:new-name /UserD:domain-username /PasswordD:*
```

- 未加入的域

```
Netdom renamecomputer %computername% /NewName:new-name
```

- 更改工作组

```
Wmic computersystem where name="%computername%" call  joindomainorworkgroup
 name="[new workgroup name]"
```

- 安装角色或可选功能

```
Start /w Ocsetup [packagename]
```


注意：对于 Active Directory，应运行具有应答文件的 Dcpromo。

- 查看角色和可选功能包名称以及当前安装状态

```
oclist
```

- 启动任务管理器热键

```
ctrl-shift-esc
```

- 注销终端服务会话

```
Logoff
```

- 设置页面文件大小
- 禁用系统页面文件管理

```
wmic computersystem where name="%computername%" set AutomaticManagedPagefile=False
```

- 配置页面文件

```
wmic pagefileset where name="C:\\pagefile.sys" set InitialSize=500,MaximumSize=1000
```

- 配置时区、日期或时间

```
control timedate.cpl
```

- 配置区域和语言选项

```
control intl.cpl
```

- 手动安装管理工具或代理

```
Msiexec.exe /i [msipackage]
```

- 列出已安装的 MSI 应用程序

```
Wmic product
```

- 卸载 MSI 应用程序

```
Wmic product get 名称/value
```

- 列出安装的驱动程序

```
Sc query type= driver
```

- 安装未包括的驱动程序，将驱动程序文件复制到服务器核心

```
Pnputil -i -a [path]\[driver].inf
```

- 重命名网络适配器

```
netsh interface set interface name="Local Area Connection" newname="PrivateNetwork"
```

- 禁用网络适配器

```
netsh interface set interface name="Local Area Connection 2" admin=DISABLED
```

- 确定文件的版本

```
wmic datafile where name="c:\\windows\\system32\\ntdll.dll" get version
```

- 已安装的修补程序列表

```
wmic qfe list
```

- 安装修补程序

```
Wusa.exe [patchame].msu /quiet
```

- 配置代理

```
Netsh winhttp set proxy [proxy_name]:[port]
```

- 添加、删除、查询注册表值

```
reg.exe add /?
reg.exe delete /?
reg.exe query /?
```

2.7.3　任务 3：更改计算机名称

① 以管理员的身份登录 Windows Server 核心服务器。

② 如图 2-79 所示，运行 HOSTNAME，显示当前计算机名称。

③ 运行 netdom RENAMECOMPUTER WIN-M95E5DFAZCO/NEWNAME:FileServer，其中 WIN-M95E5DFAZCO 是现在的计算机名称，FileServer 是新的计算机名称。

④ 如图 2-79 所示，运行 shutdown /r /t 0，重启系统。

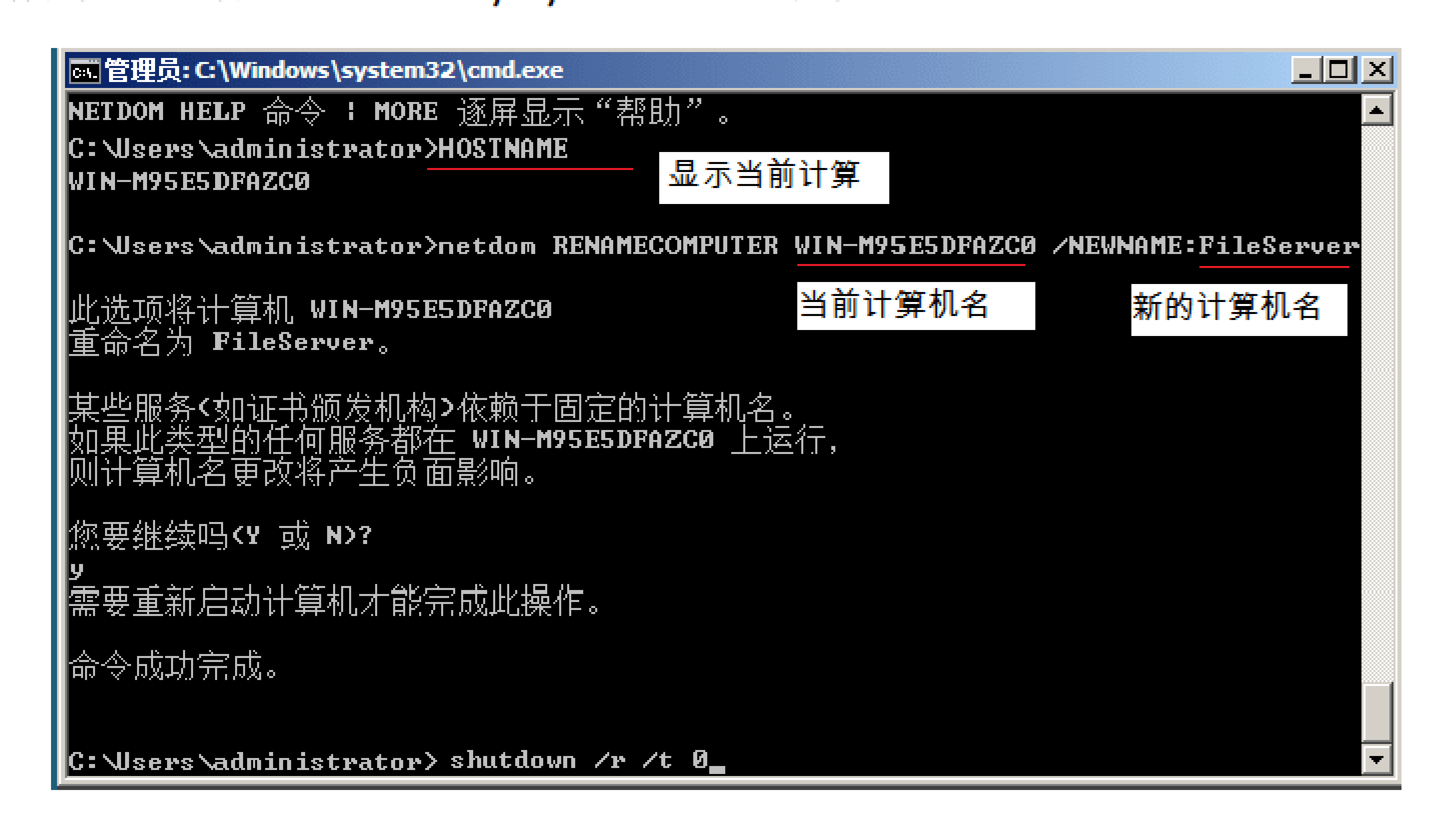


图 2-79　查看和更改计算机名称

2.7.4　任务 4：配置网络连接

① 使用管理员账户登录 Windows Server 核心操作系统。

② 使用 ipconfig /all 查看 IP 地址。如图 2-80 所示，发现已经从 DHCP 请求得到了地址。

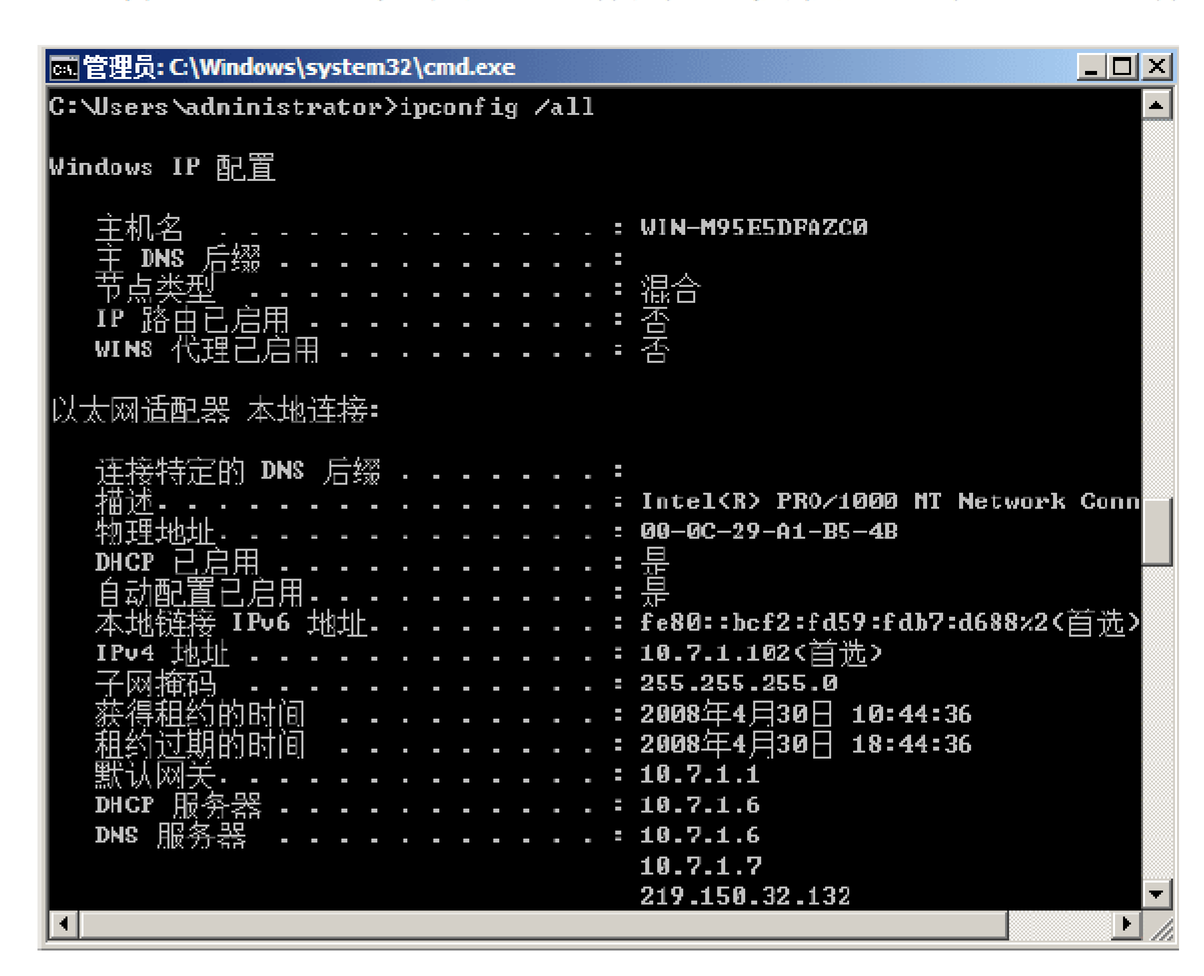


图 2-80　查看本地连接的 IP 设置

③ ping www.inhe.net 测试到 Internet 的连接性。如图 2-81 为测试域名解析和网络连通性。发现能够解析该域名的地址，并且能够从该地址返回数据包。

1. 手工指定静态地址

如果网络上没有为 DHCP 服务器分配 IP 地址，则需要进行以下人工指定静态地址的步骤，如图 2-82 所示。

① 输入 netsh。
② 输入 interface。
③ 输入 show interface，显示接口。
④ 输入 Exit，退出。

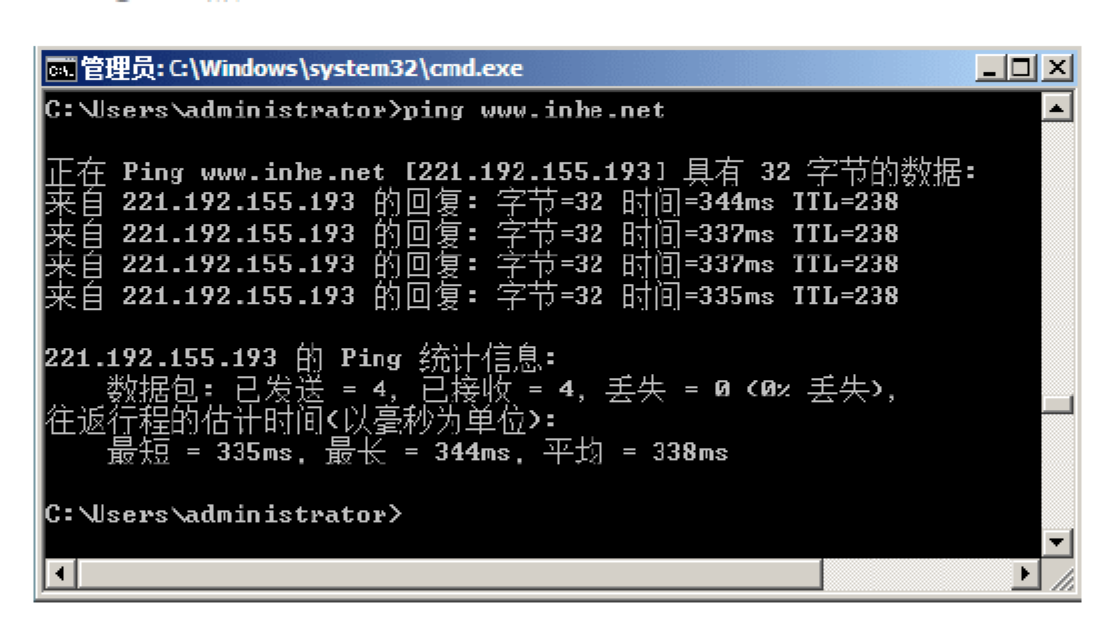


图 2-81 测试域名解析和网络连通

```
C:\Windows\system32>netsh
netsh>interface
netsh interface>show interface

管理员状态     状态          类型          接口名称
---------------------------------------------------
启用           已连接上      专用          本地连接

netsh interface>
```

图 2-82 查看本地连接状态

⑤ 输入 netsh。
⑥ 如图 2-83 所示，输入 interface ipv4 set address name=“本地连接”source=static addr=10.7.1.212 mask= 255.255.255.0 gateway=10.7.1.1。

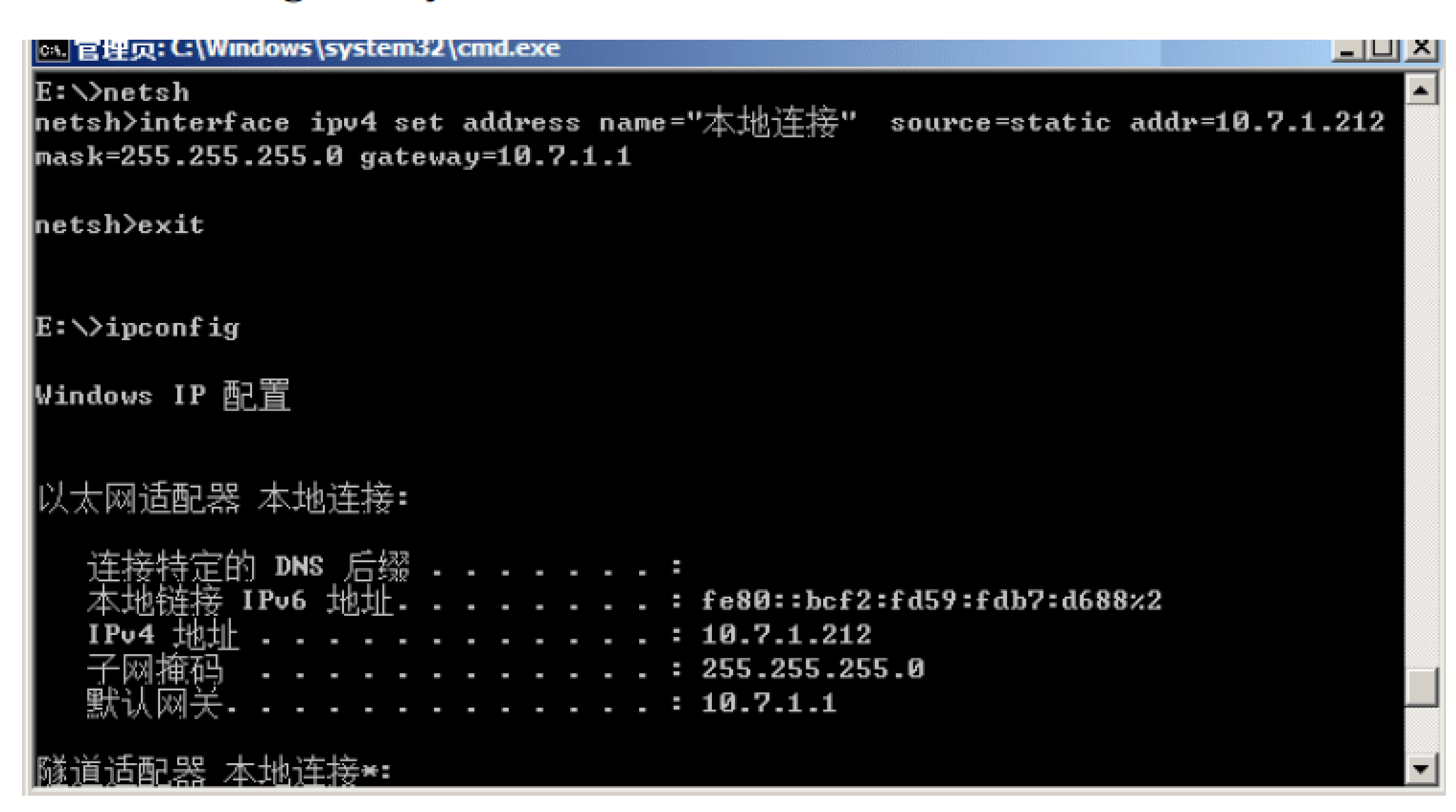


图 2-83 更改 IP 地址

2. 配置指定使用的 DNS 服务器

① 输入 netsh。
② 如图 2-84 所示，输入 interface ipv4 set dnsserver “本地连接” static 202.99.160.68 primary。
③ 输入 Exit，退出。
④ 输入 ipconfig /all，查看配置的 DNS。
⑤ Ping www.inhe.net 测试到 Internet 的连接性。发现能够解析该域名的地址，并且能够从该地址返回数据包。这表明能够连接到 Internet。

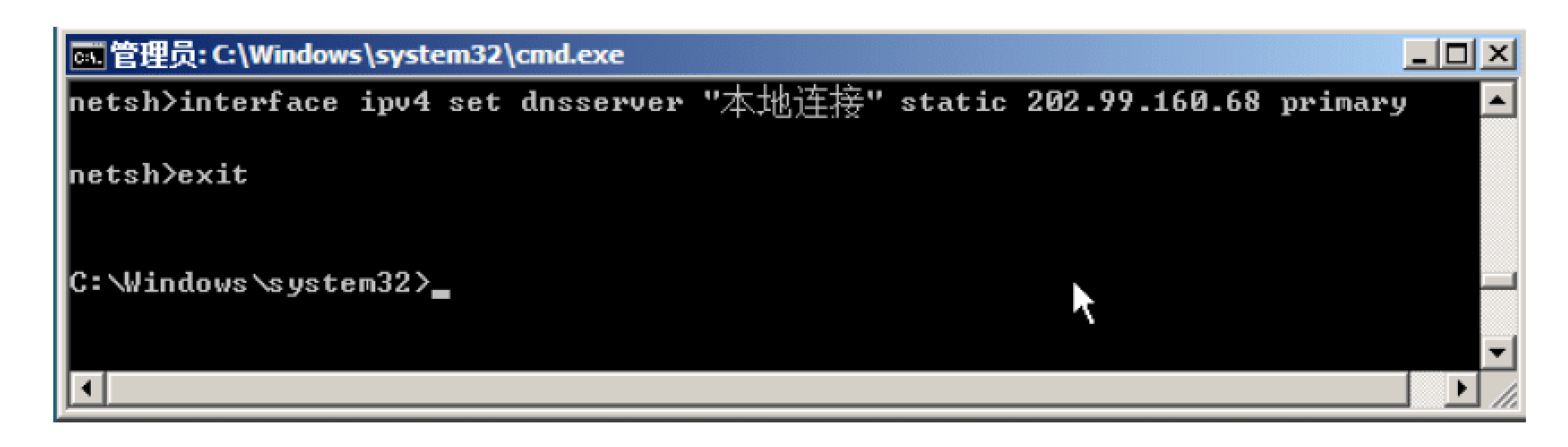


图 2-84　指定首选的 DNS 服务器

2.7.5　任务 5：激活服务器

① 如图 2-85 所示，运行 slmgr -xpr，查看操作系统过期时间。

② 如图 2-86 所示，更改产品密钥，在命令行输入：slmgr -ipk YK333-24HJX-JDR2Y-B8KPY-4R7KY。

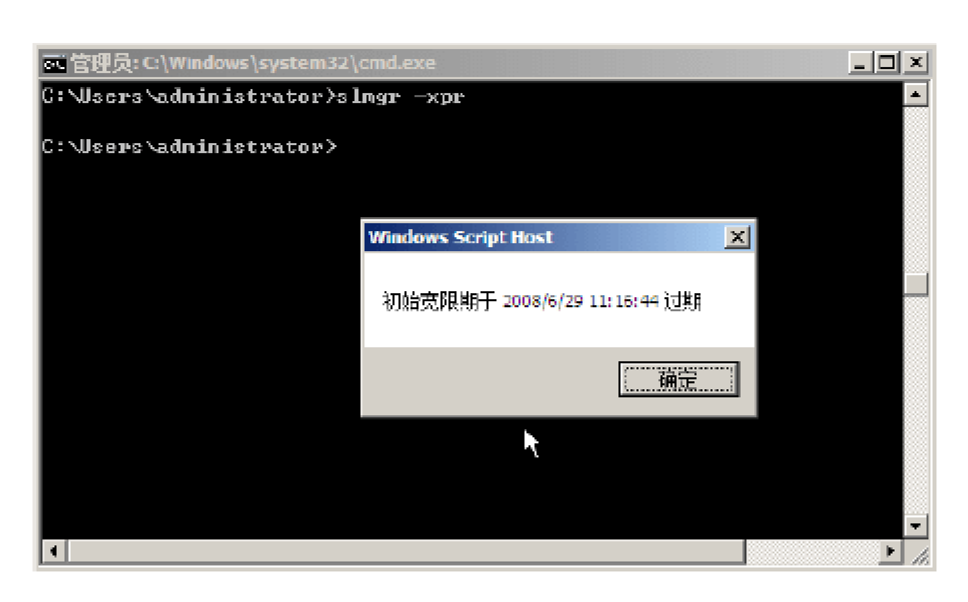


图 2-85　查看过期时间

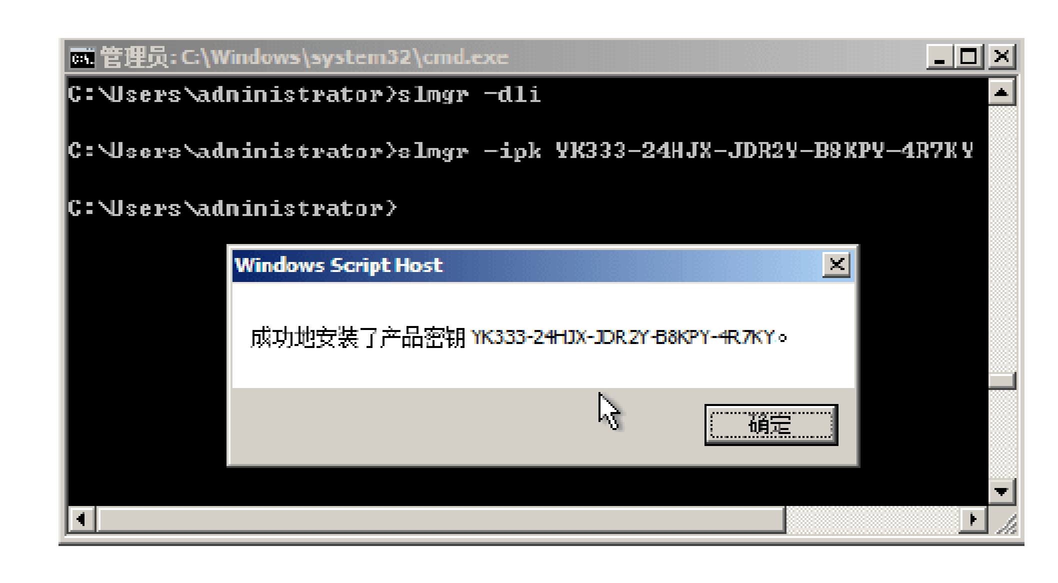


图 2-86　更改产品密钥

③ 如图 2-87 所示，运行 slmgr -ato，激活服务器。

④ 如图 2-88 所示，再次查看授权信息，发现已授权。

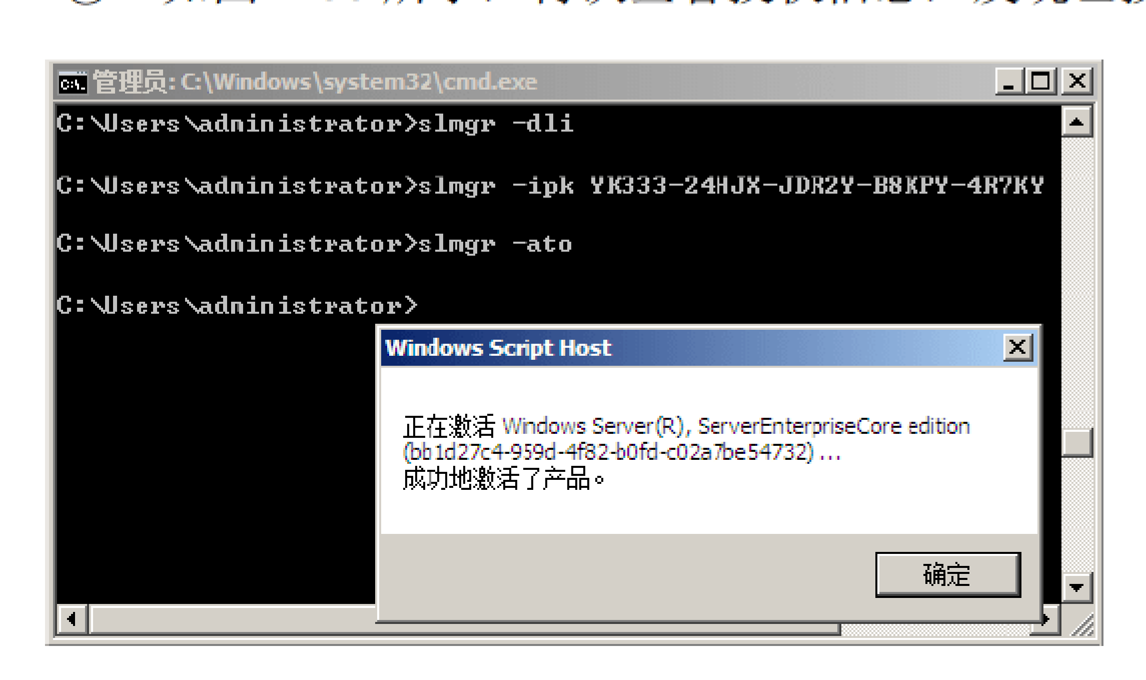


图 2-87　激活成功

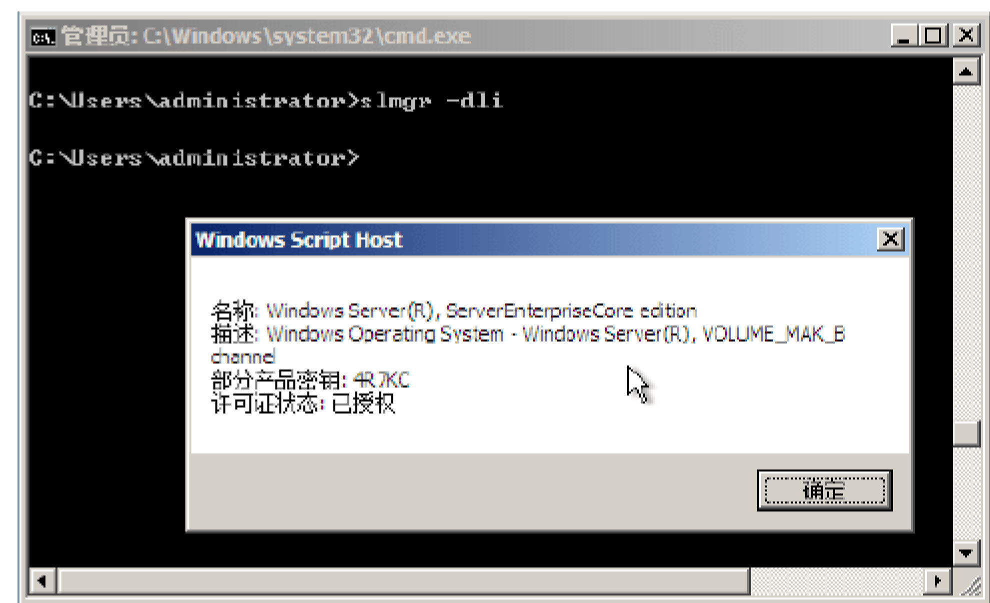


图 2-88　显示已授权

2.8　实战：使用 Windows PE 备份和还原系统

任务描述

在企业实际的应用环境中，关键业务所使用的操作系统大多不用虚拟机，为了防止操作系统失败造成的不可用，使用磁盘备份软件 Ghost，可以将运行正常的操作系统的系统分区备份到其他分区，这样一旦

操作系统由于病毒或其他原因启动失败，我们就可以使用以前的备份迅速还原。

使用 Windows PE 引导进入系统，备份系统和还原系统，并且能够使用 Windows PE 光盘清除管理员密码，以及能够在操作系统意外失败的情况，使用 Windows PE 进入系统复制出重要数据。能够使用 Windows PE 找到删除的文件。

实战环境

- 一台装好 Windows Server 2008 的服务器
- 该服务器必须有两个分区
- 带 Ghost 的 Windows PE 引导盘

实战目标

- 能够使用 Ghost 软件备份和还原操作系统
- 能够清除管理员密码

2.8.1 任务 1：备份操作系统

将系统盘备份到其他分区，要求系统必须至少有两个分区。下面的操作先创建新的分区，再从 Windows PE 引导，备份系统到第二个分区。

① 单击 按钮启动虚拟机，以管理员身份登录。

② 打开服务器管理器，选择“存储”→“磁盘管理”命令。

③ 如图 2-89 所示，右击磁盘 0 未分配空间，单击“新建简单卷”按钮。

④ 如图 2-90 所示，指定分区大小，单击“下一步”按钮。

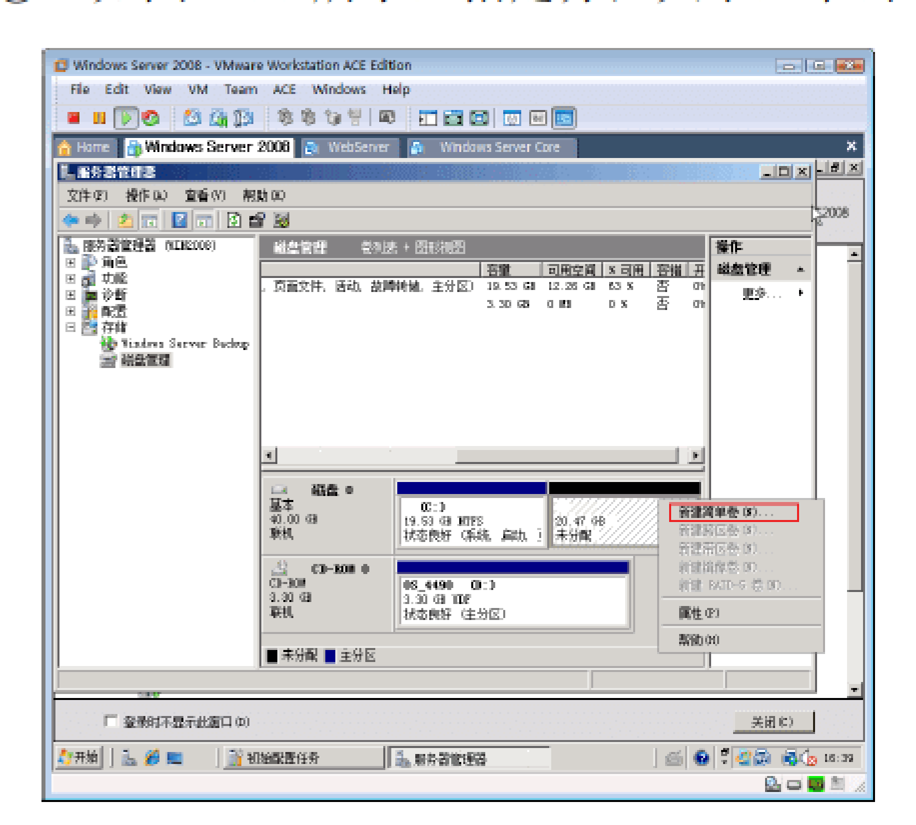


图 2-89 创建简单卷

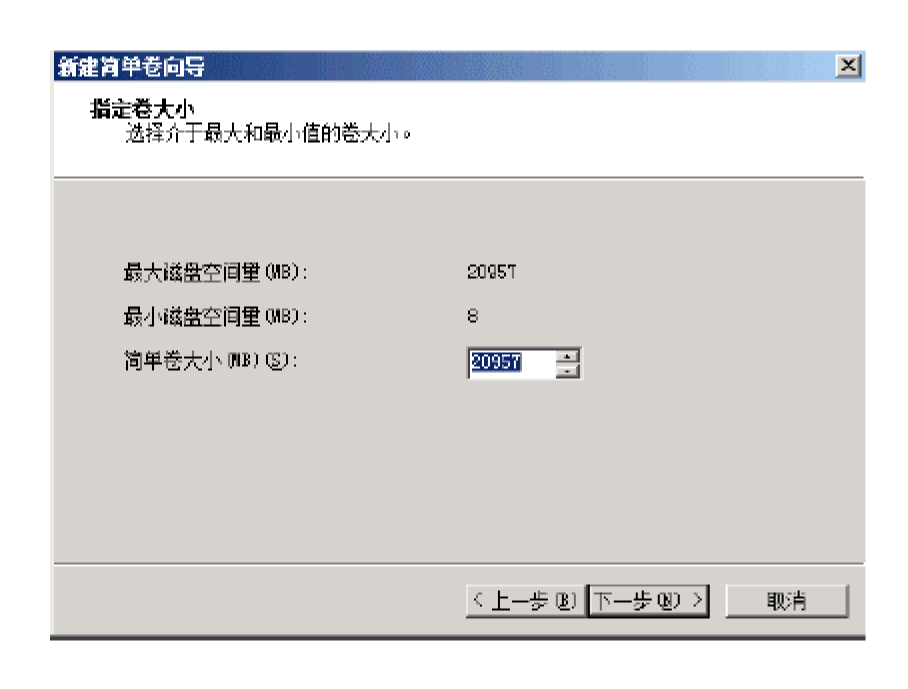


图 2-90 指定磁盘大小

⑤ 如图 2-91 所示，指定驱动器号，单击“下一步”按钮。

⑥ 如图 2-92 所示，“文件系统”为 NTFS，选中“执行快速格式化”复选框，单击“下一步”按钮，单击“完成”按钮。

关闭虚拟机

如果你将整个盘作为一个分区安装了操作系统，则需要关闭虚拟机，添加一块新的磁盘，然后开机格式化一个新的卷。

① 如图 2-93 所示，单击 CD-ROM 图标，浏览到 Windows PE ISO 文件后，单击 OK 按钮。

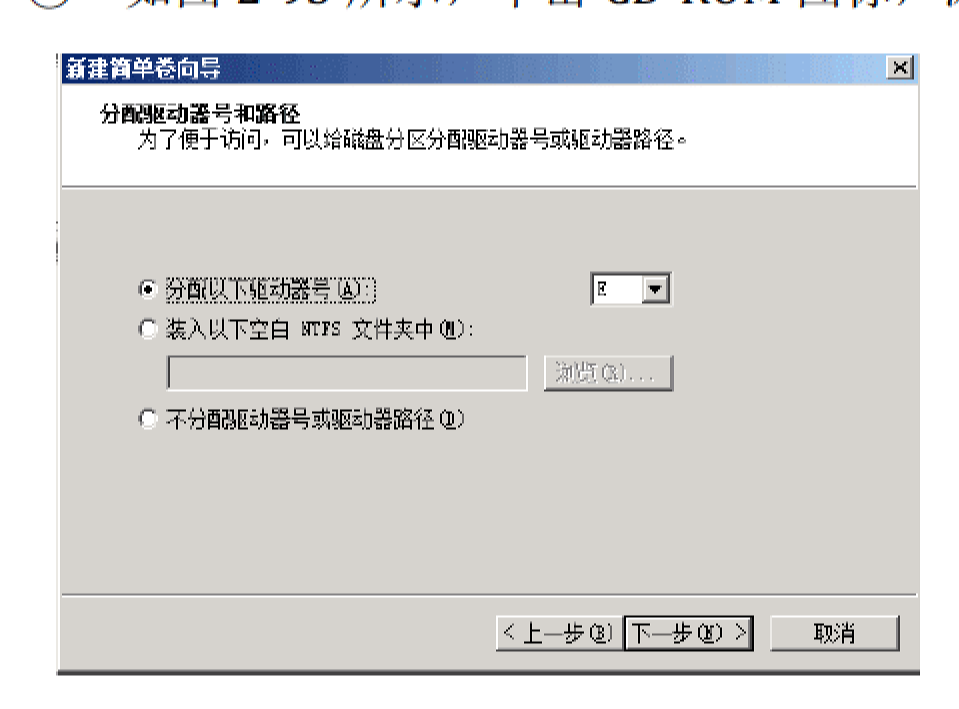


图 2-91　指定盘符

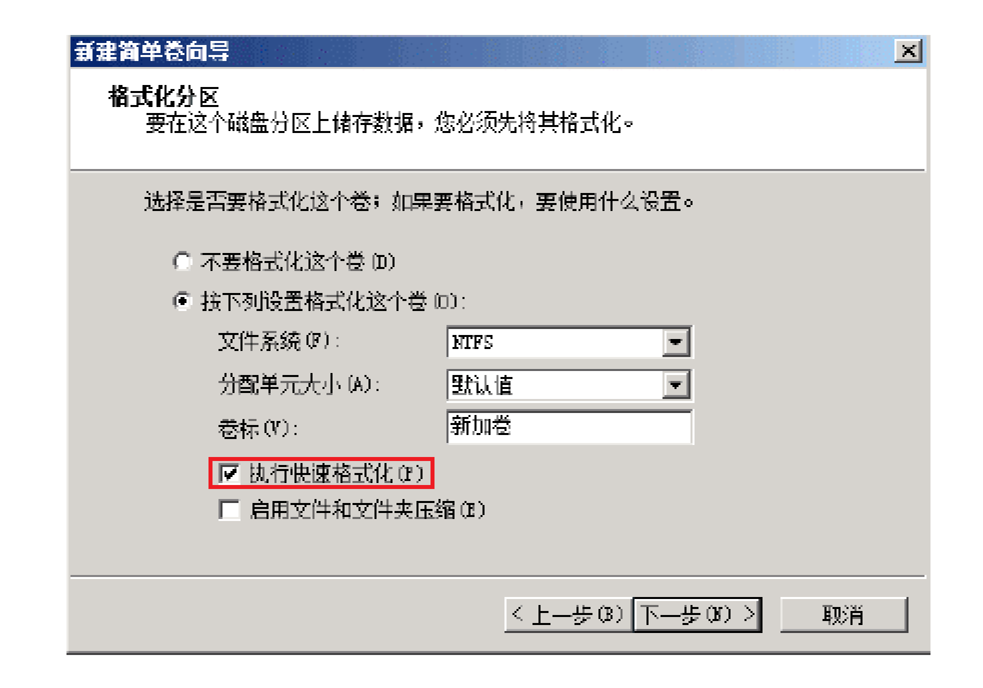


图 2-92　格式化分区

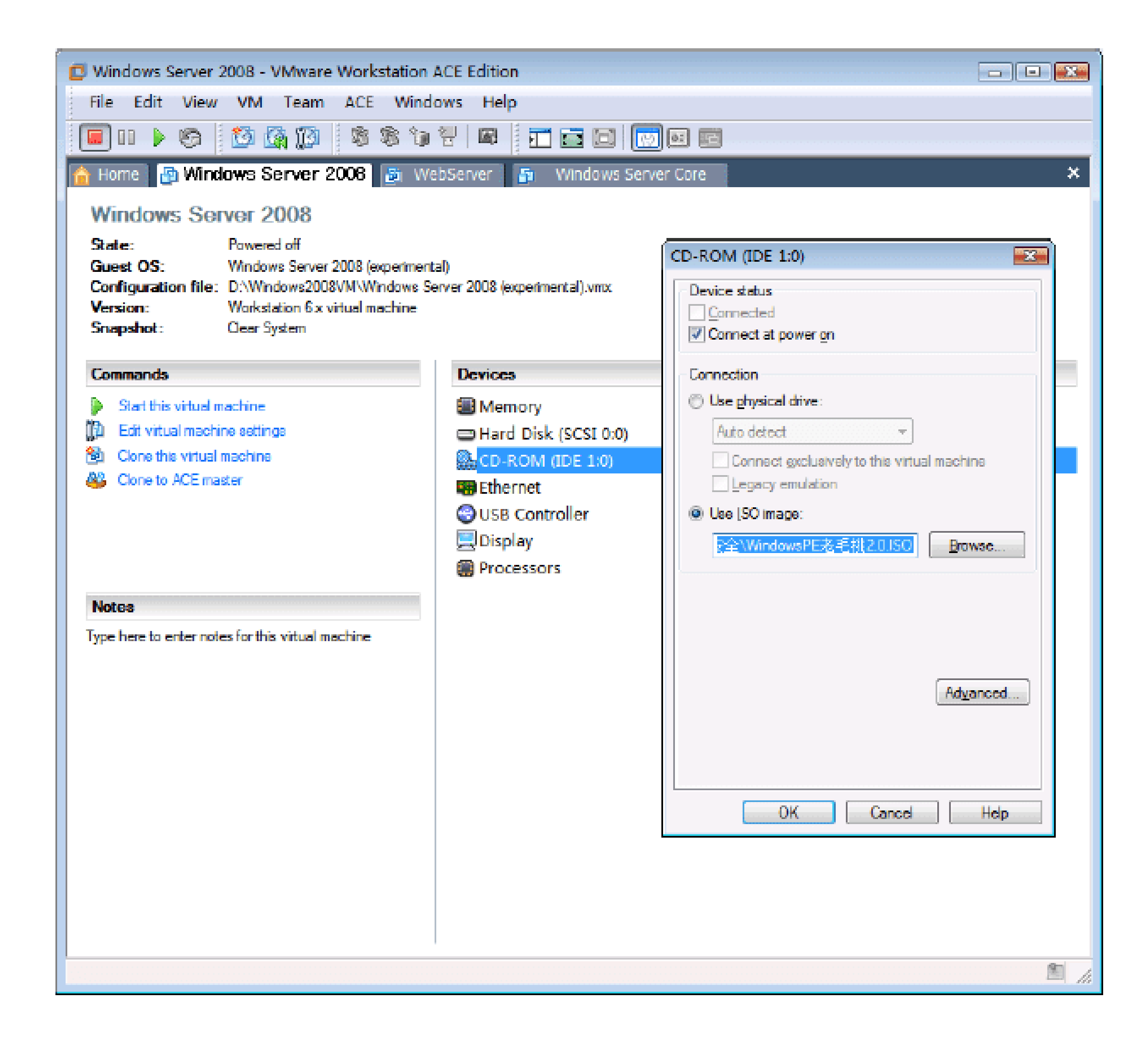


图 2-93　插入 Windows PE 安装盘

② 启动虚拟机，将光标点进虚拟机，在出现下图界面时，按 F2 键，进入 BIOS 设置，如图 2-94 所示，设置引导顺序。按“-”、“+”键调整顺序，将 CD-ROM Driver 调整到最高，按 F10 键，保存退出。

③ 如图 2-95 所示，重启系统，进入 Windows PE 界面(貌似 Windows XP 的图形界面)。

④ 进入系统后，选择“开始”→“程序”→“克隆工具”→“诺顿 ghost32 v 11”命令。如图 2-96 所示，选择 load→partition→ToImage 命令。将 C 分区备份为一个扩展名为 gho 的文件。

⑤ 如图 2-97 所示，选择要备份的分区位于第几块硬盘上。因为这个计算机就一块硬盘，选中该盘，单击 OK 按钮。

⑥ 如图 2-98 所示，选择要备份的分区，单击 OK 按钮。

⑦ 如图 2-99 所示，指定备份存储位置，并指定文件名。

⑧ 如果将备份指定到第一块盘的第二个分区，单击 Save 按钮。如图 2-100 所示，在弹出的对话框中单击 High 按钮，这样占用磁盘空间小。

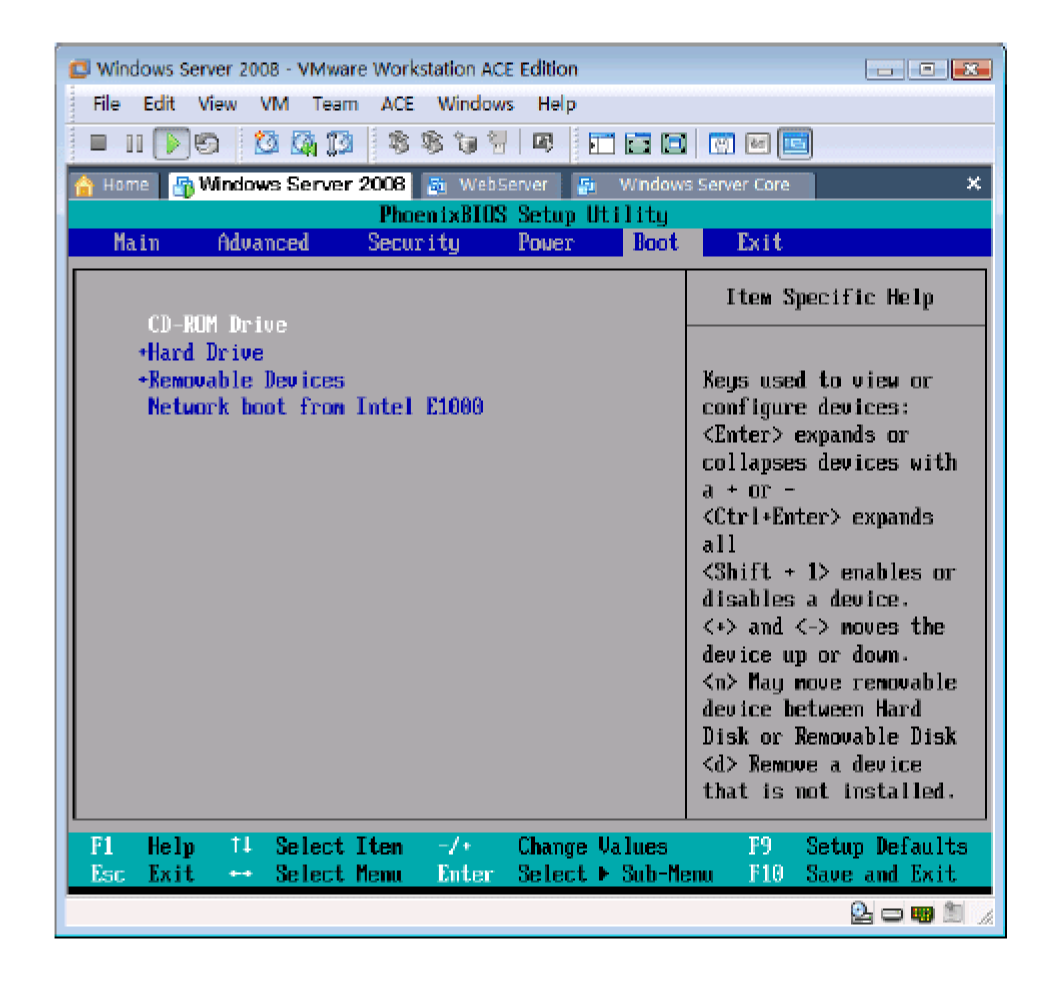


图 2-94 设置引导顺序

图 2-95 进入 Windows PE

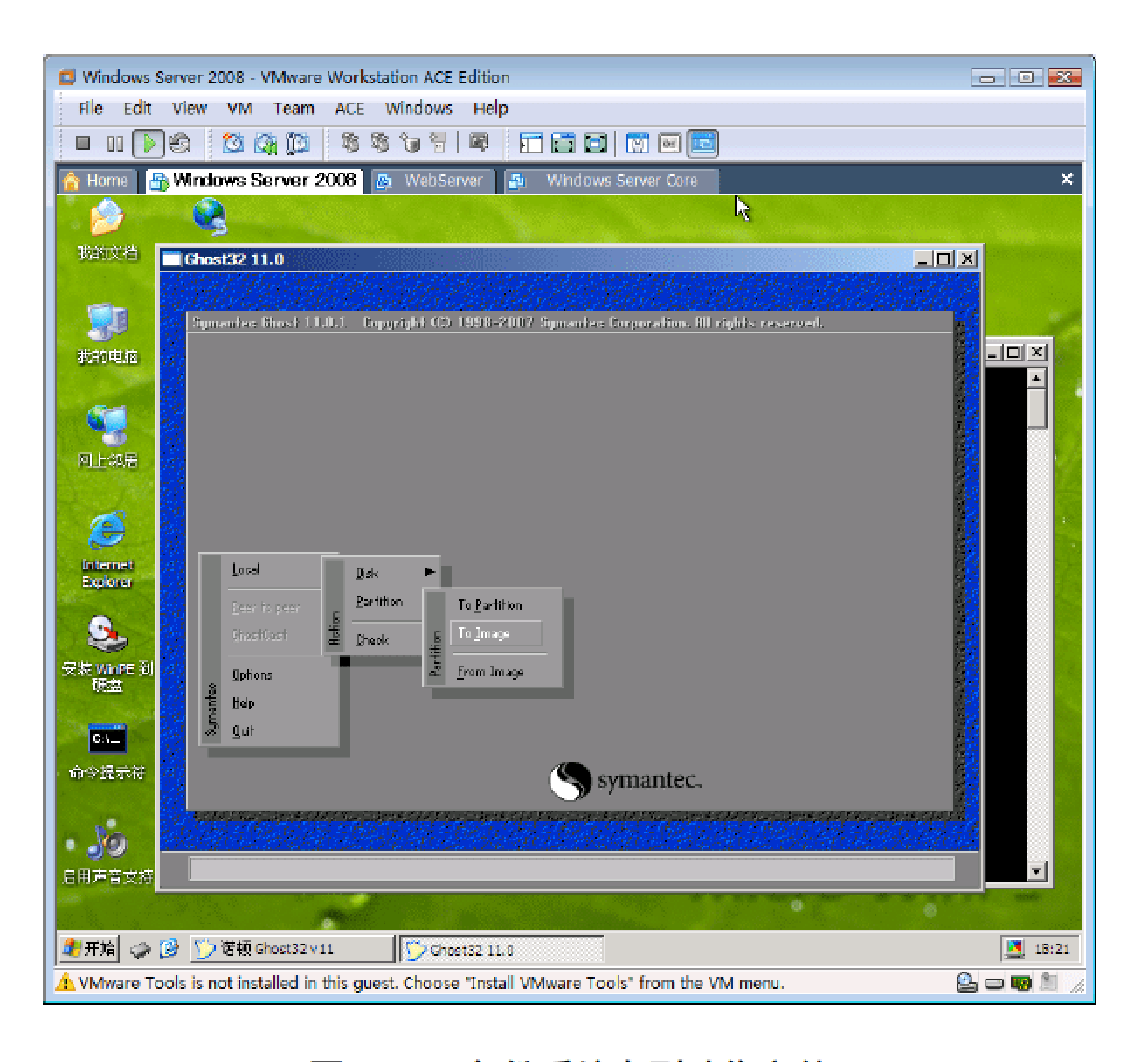
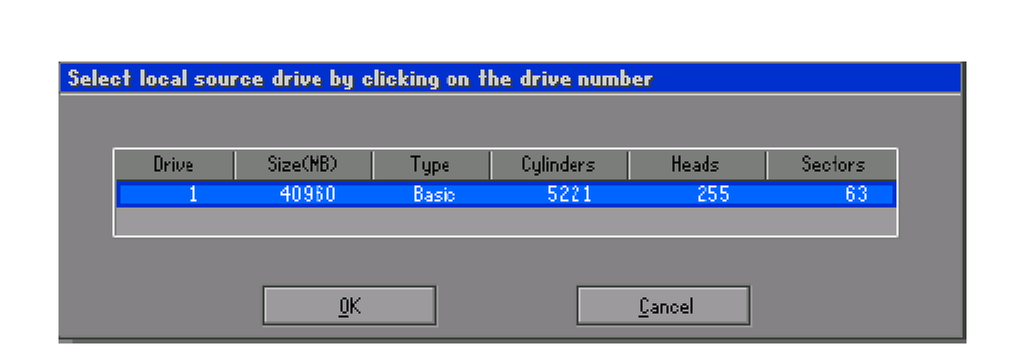


图 2-96 备份系统盘到映像文件



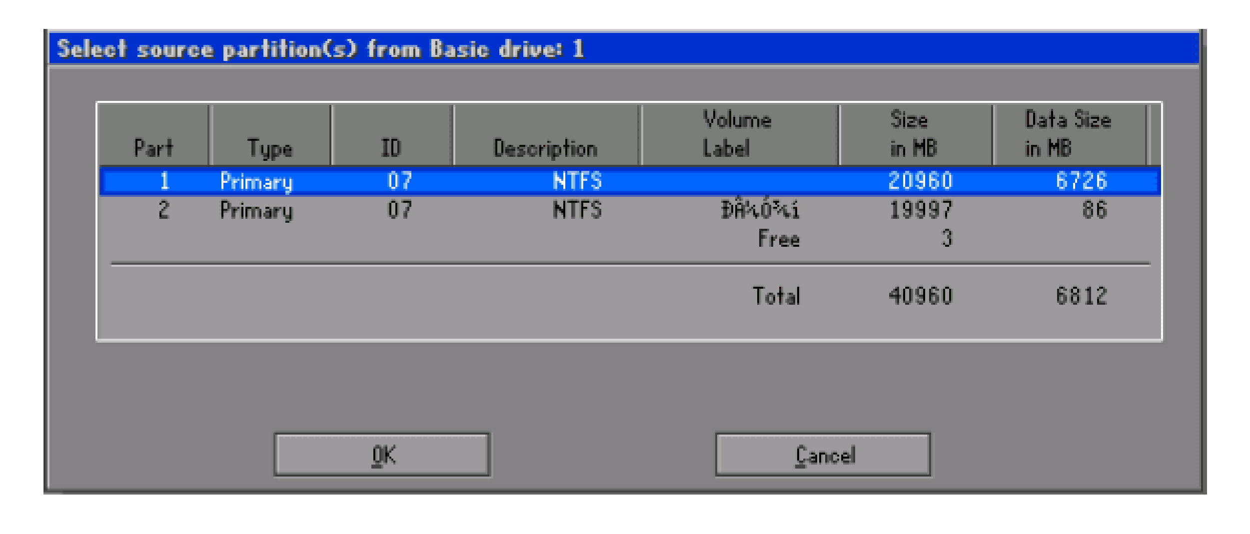


图 2-97 选择要备份的磁盘

图 2-98 选择要备份的分区

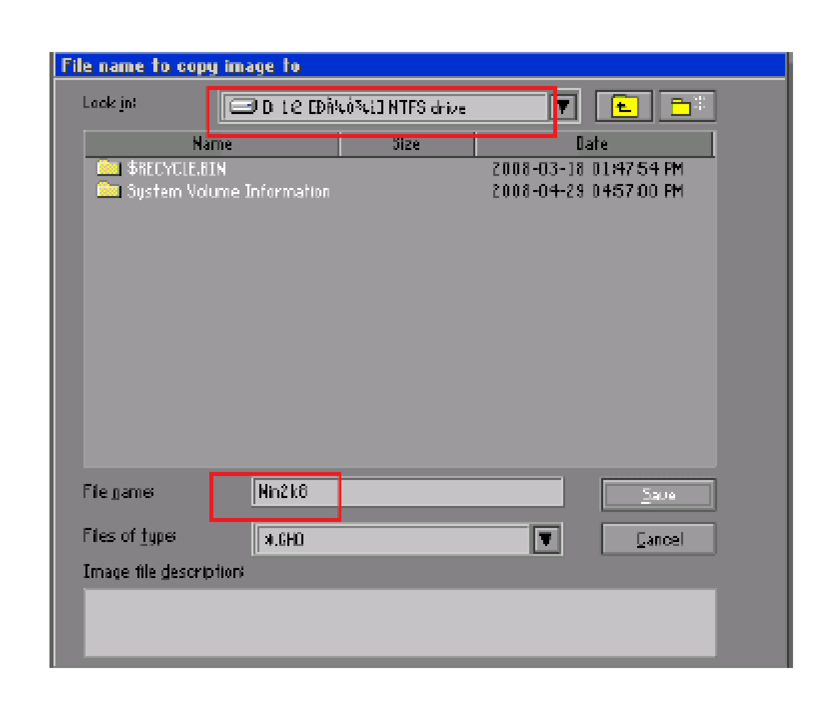


图 2-99　指定备份存储位置

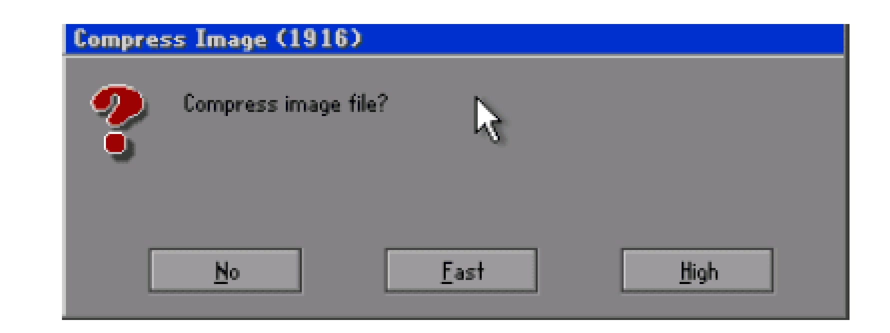


图 2-100　指定是否压缩



提示：No 就是不压缩，最快的速度；Fast 就是低压缩，较快的速度；High 就是高压缩，较慢的速度。

⑨　备份完成后，单击 Continue 按钮，单击 Quit 按钮，退出备份。

2.8.2　任务 2：还原操作系统

①　使用 Windows PE 引导进入系统。

②　进入系统后，单击“开始”→“程序”→“克隆工具”→“诺顿 ghost32”命令。

③　如图 2-101 所示，选择 load→partition→From Image 命令。

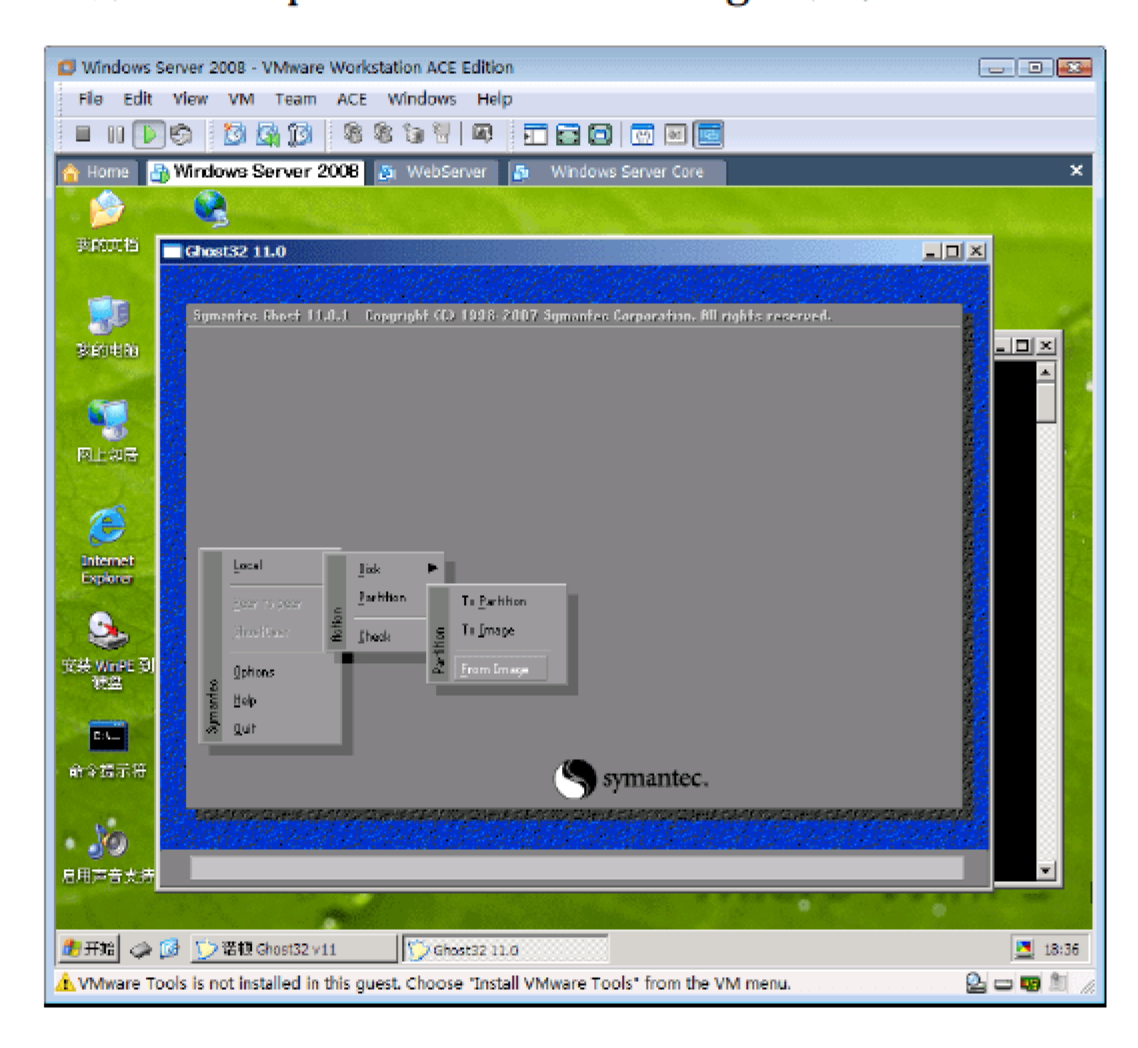


图 2-101　还原系统

④　如图 2-102 所示，选择备份的 ghost 文件。

⑤　如图 2-103 所示，选择源分区，单击 OK 按钮。

⑥　如图 2-104 所示，选择要还原到的目标磁盘。

⑦　如图 2-105 所示，指定目标磁盘上的目标分区，单击 OK 按钮。

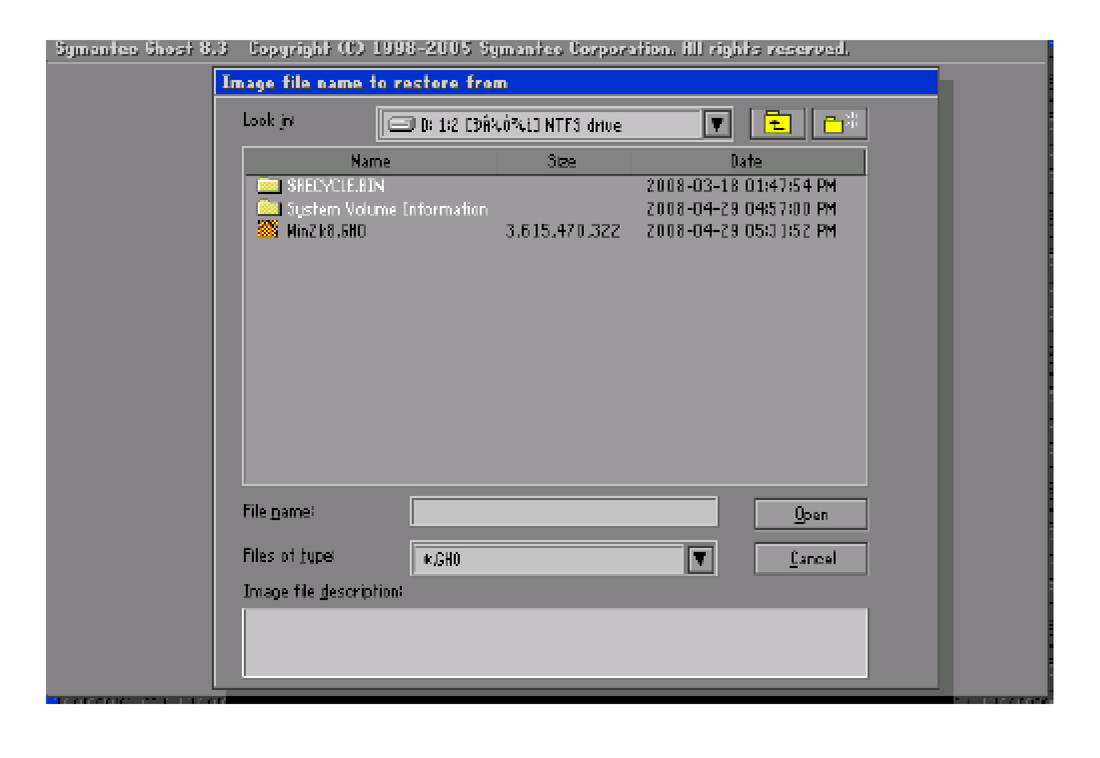


图 2-102　选择系统备份文件

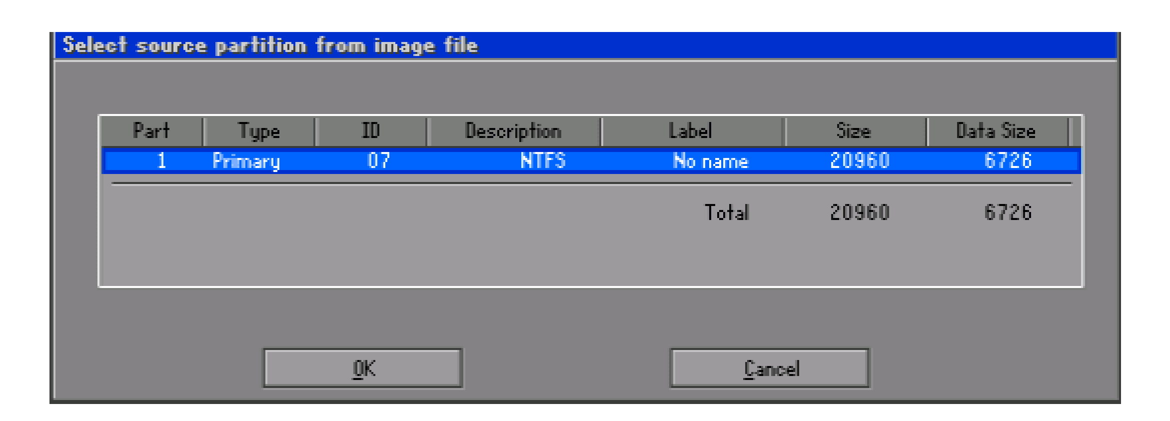


图 2-103　选择源分区

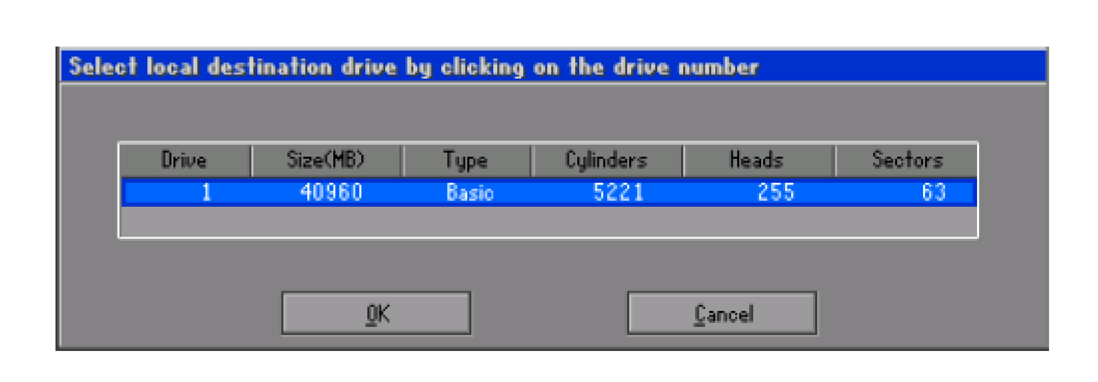


图 2-104　选择目标磁盘

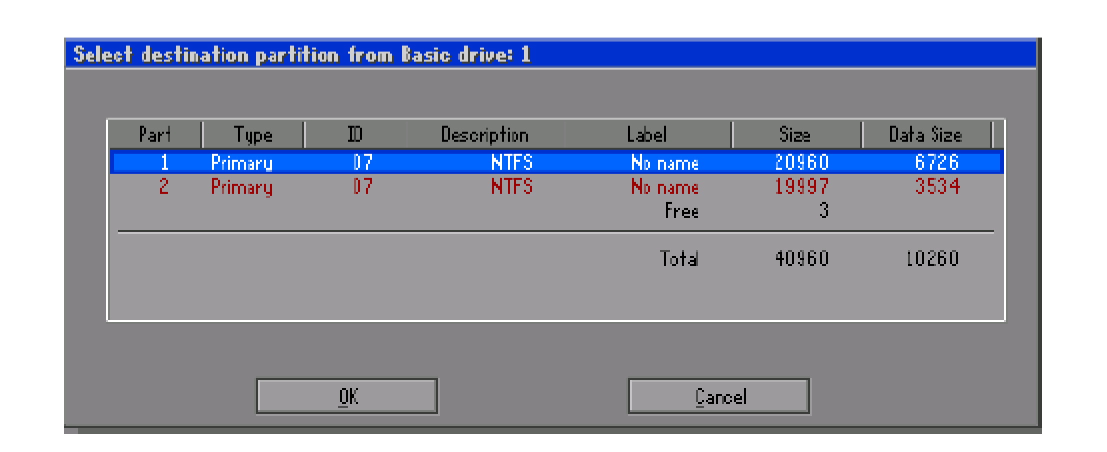


图 2-105　选择目标分区

⑧　如图 2-106 所示，在弹出的提示框中单击 Yes 按钮。

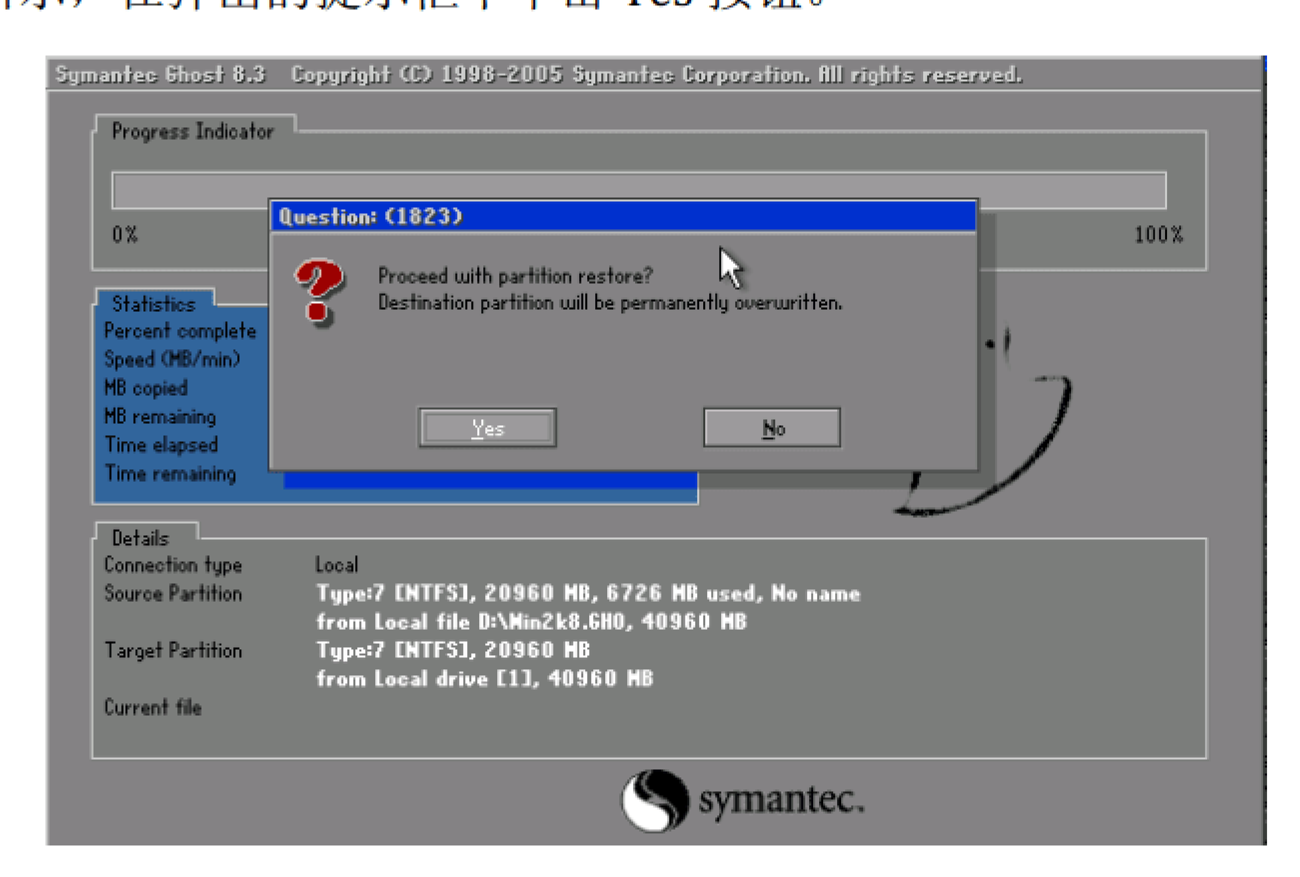


图 2-106　还原前的提示框

⑨　还原完成后，关机，取出光盘，启动系统。

2.8.3　任务 3：重新设置密码

当用户忘记或不知道系统管理密码时可以无条件重设任何用户密码。

①　使用 Windows PE 引导系统。

②　选择“开始”→“程序”→“Windows 系统维护”→“Windows 用户密码维护”命令，如图 2-107 所示，打开用户密码恢复工具。



图 2-107　用户密码恢复工具

③　如图 2-108 所示，单击“选择目标路径”按钮。浏览到装有系统的目录 C:\Windows。



图 2-108　选择系统目录

④　单击“修改现有用户的密码”按钮。

⑤　如图 2-109 所示，单击“用户名”下拉列表框右侧的下三角按钮，则能看到该计算机中的所有用户。

⑥　选中用户，直接输入新密码，然后单击“应用”按钮。

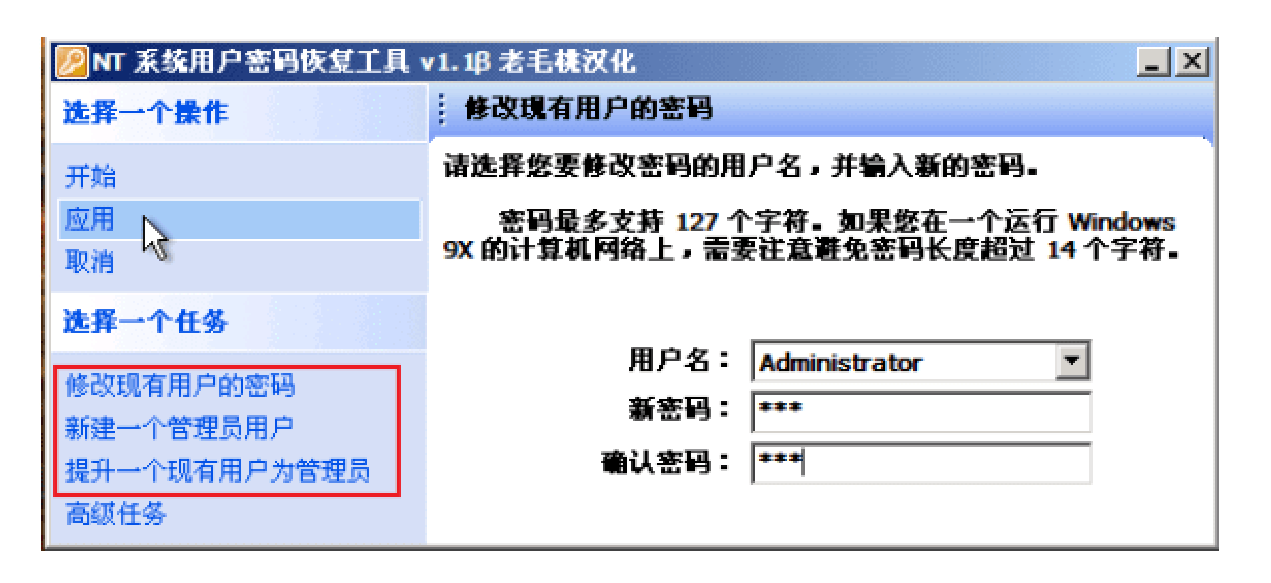


图 2-109　重设管理员密码

⑦　用户可以新建一个管理员用户，也可以提升一个现有用户为管理员。

2.8.4　任务 4：恢复删除的文件

误删除之后，第一件事就是恢复数据，如果又在该分区存放了新的文件，则有可能覆盖了删除的文件，此时，可能就不能完整恢复整个文件，或根本就恢复不了。

万一不小心彻底删除了不该删除的文件，不要在该分区盘上复制任何新文件，可从 Windows PE 引导，进入系统，恢复删除的文件。

① 使用 Windows PE 引导系统。

② 选择“开始”→“程序”→“文件工具”→文件恢复 FinalData 命令。

③ 如图 2-110 所示，单击图标，选择删除的文件所在磁盘，单击“确定”按钮。

④ 如图 2-111 所示，选择要搜索的簇范围。单击“确定”按钮。

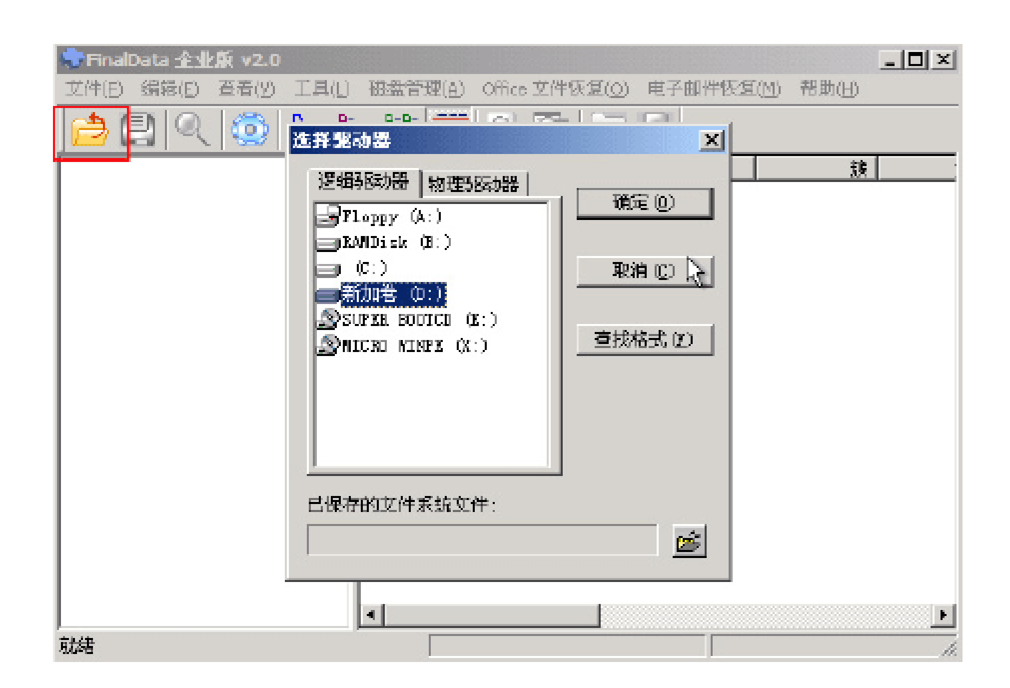


图 2-110　指定删除的文件所在的磁盘



图 2-111　指定要搜索的簇范围

⑤ 扫描完成之后，找到已经删除的文件后右击，在弹出的快捷菜单中选择“恢复”命令。

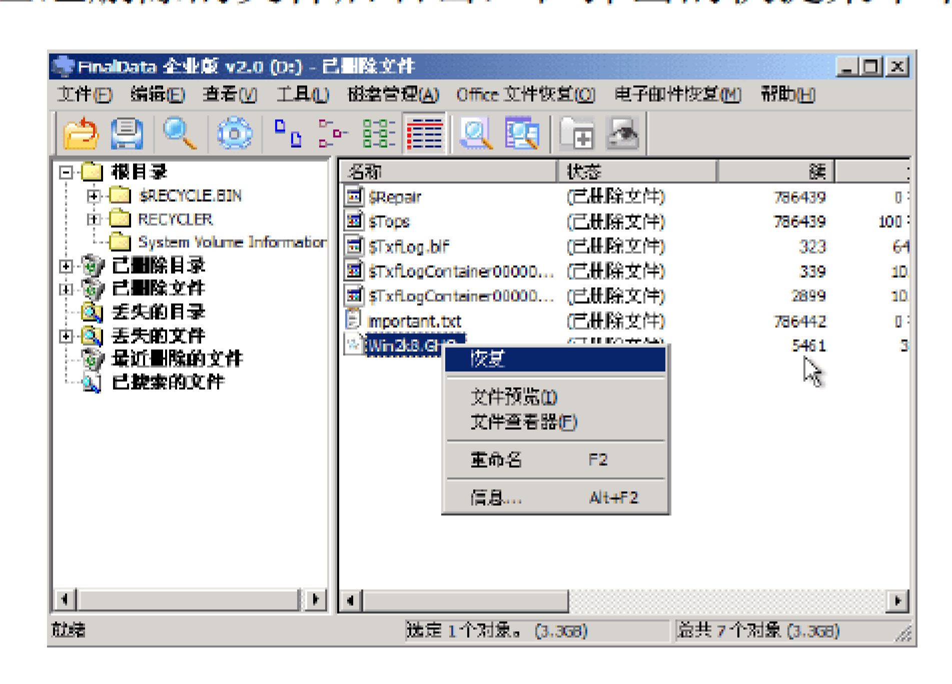
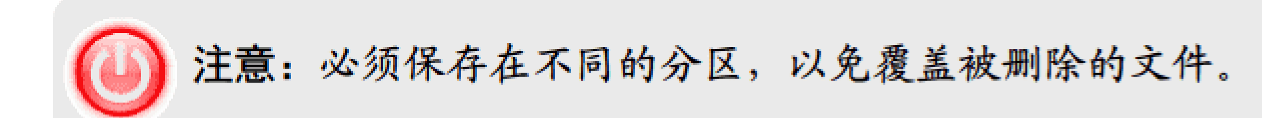


图 2-112　找到删除的文件

⑥ 如图 2-113 所示，恢复到其他分区。最后单击“保存”按钮。



注意：必须保存在不同的分区，以免覆盖被删除的文件。

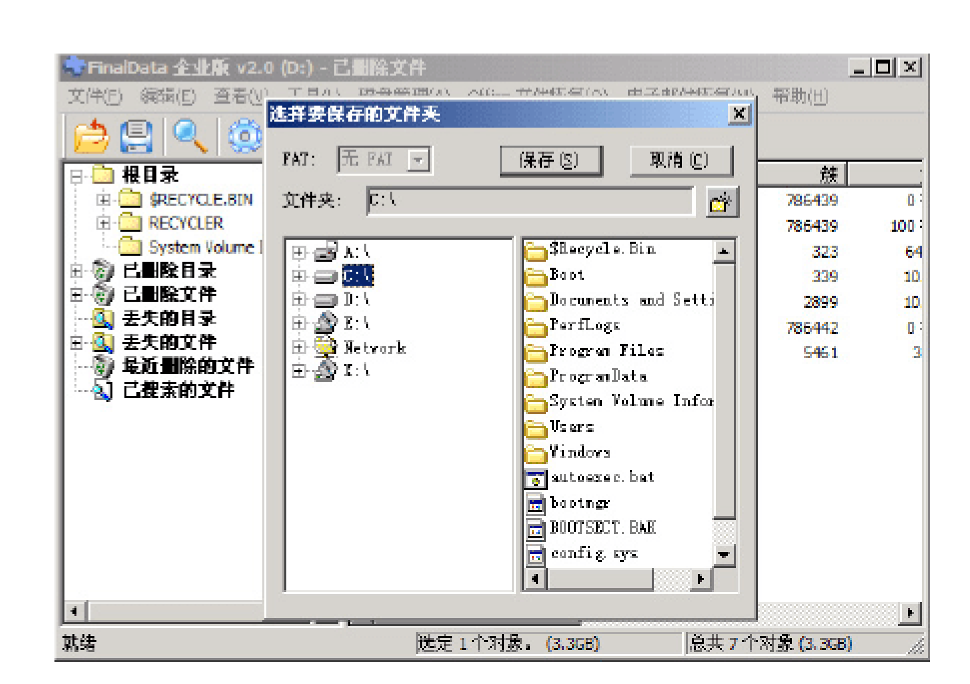


图 2-113　恢复到其他分区

第 3 章　配置 Windows Server 2008 环境

Windows Server 2008 中的角色和功能，相当于 Windows Server 2003 中 Windows 组件，重要的组件划分到了 Windows Server 2008 角色，不太重要服务和增加服务器的功能划分到了 Windows Server 2008 功能。

服务器管理器提供了完成服务器所有的管理工作的界面，包括添加删除角色和功能，更改计算机属性，存储管理，用户管理，日志管理等。

关键词

- 服务器功能和角色介绍
- 使用服务器管理器管理服务器
- 配置和管理硬件
- 定义用户桌面环境
- 配置 IE 选项
- 配置反间谍软件 Windows Defender
- 配置网络中心
- 配置本地连接
- 常用网络排错工具

3.1 服务器角色、角色服务和功能

本部分定义适用于 Windows Server 2008 的术语：角色、角色服务和功能。

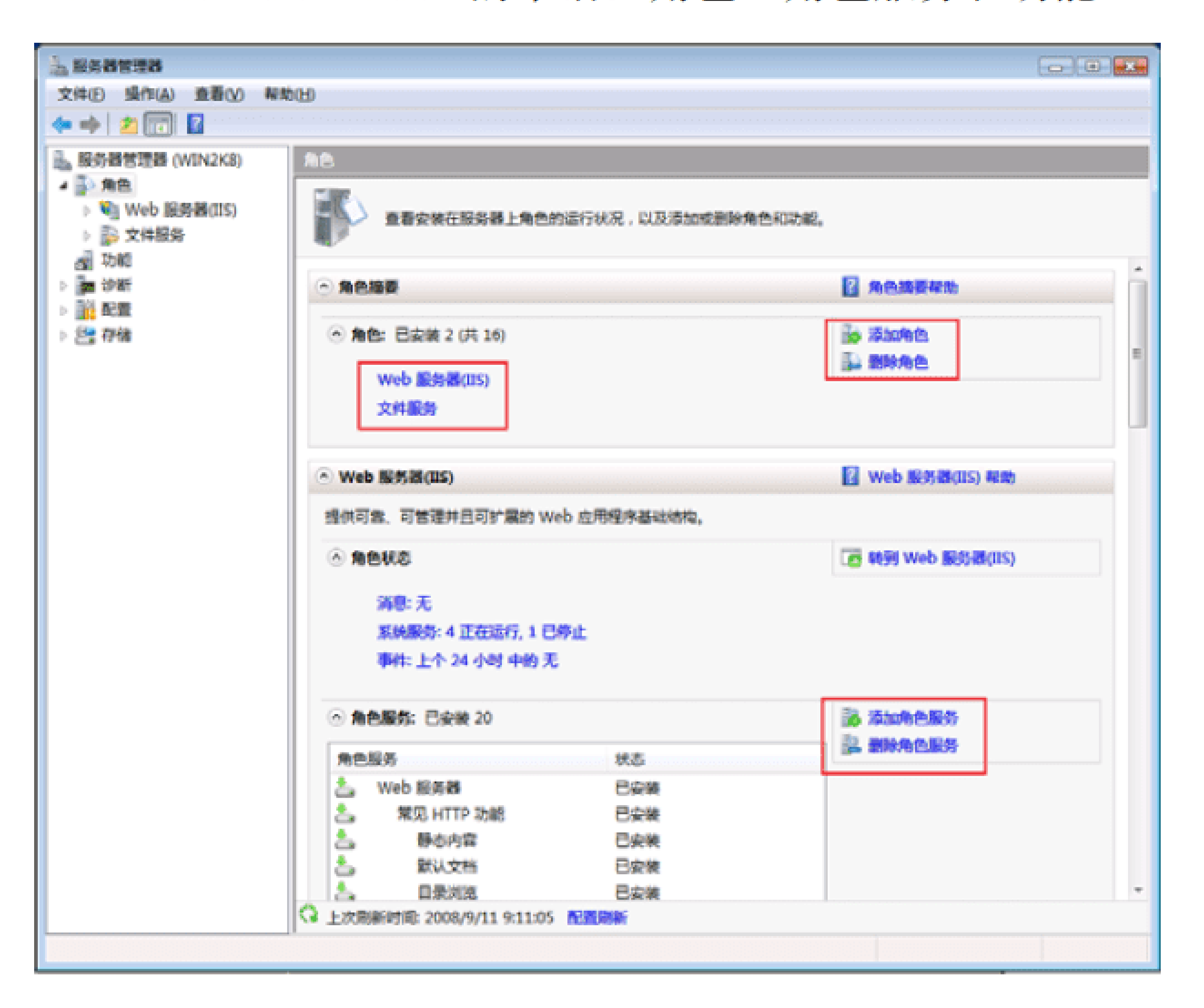


图 3-1 服务器角色、角色服务以及功能

3.1.1 角色

Roles 是出现在 Windows Server 2008 中的一个新概念，也是 Windows Server 2008 管理特性中很重要的一个亮点。如何理解 Roles 呢？字面指的是角色，这里指的是服务器角色，或者指的是运行某一个特定服务的服务器角色。当一台服务器安装了某个服务后，其实就是赋予了这台服务器一个角色，这个角色的任务就是为应用程序、计算机或者整个网络环境提供该项服务。

服务器角色是软件程序的集合，在安装并正确配置之后，允许计算机为网络内的多个用户或其他计算机执行特定功能。一般来说，角色具有下列共同特征。

- 角色描述计算机的主要功能、用途或使用。特定计算机可以专用于执行企业中常用的单个角色，如果多个角色在企业中均很少使用，则还可以执行多个角色。
- 角色允许整个组织中的用户访问由其他计算机管理的资源，比如网站、打印机或存储在不同计算机上的文件。
- 角色通常包括自己的数据库，这些数据库可以对用户或计算机请求进行排队，或记录与角色相关的网络用户和计算机的信息。例如，Active Directory 域服务包括一个用于存储网络中所有计算机的名称和层次结构关系的数据库。

正确安装并配置角色之后，将角色设置为自动工作，以允许安装此角色的计算机，图 3-2 显示了 Windows Server 2008 的所有角色。表 3-1 是角色描述。

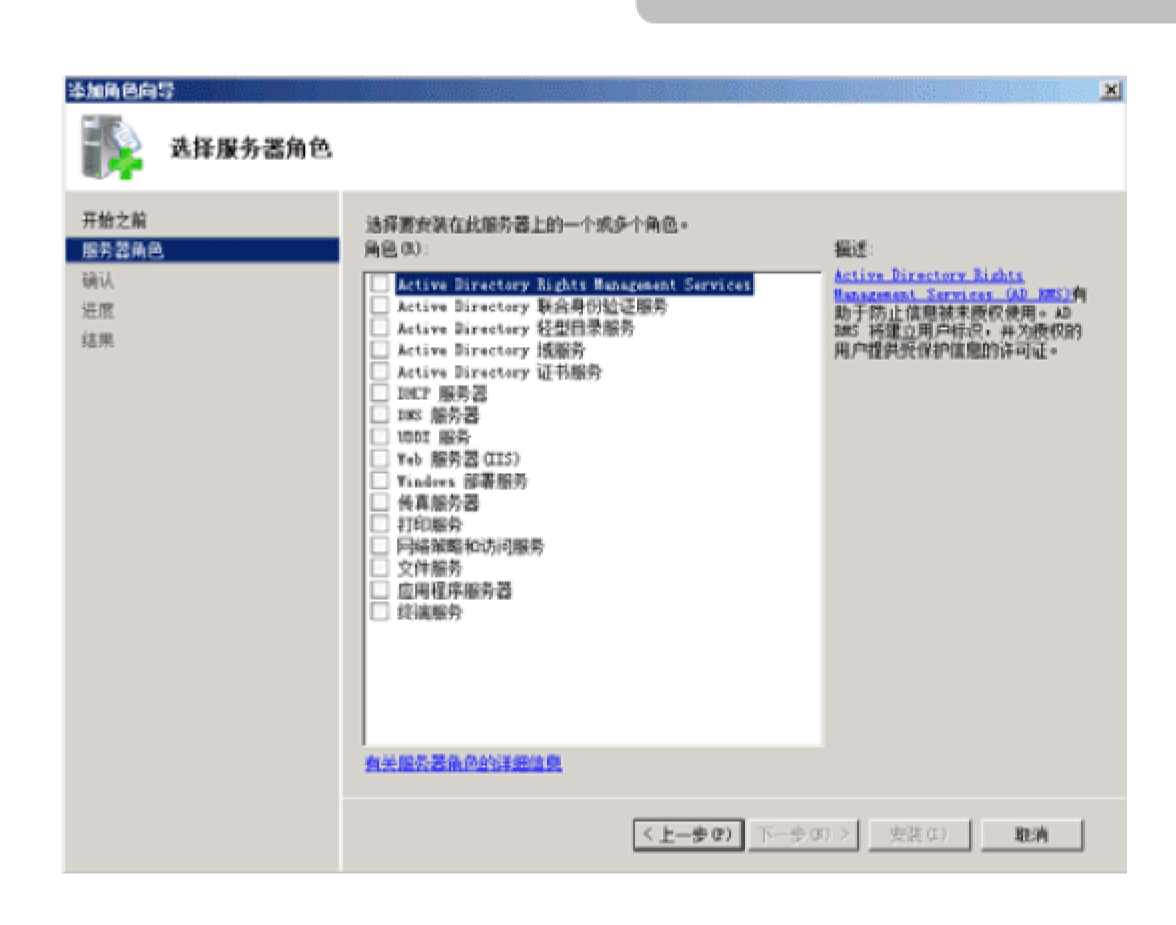


图 3-2　Windows Server 2008 服务器角色

表 3-1　角色描述

角色名称	描　述
Active Directory 证书服务	Active Directory 证书服务提供可自定义的服务，用于创建并管理在采用公钥技术的软件安全系统中使用的公钥证书。组织可使用 Active Directory 证书服务通过将个人、设备或服务的标识与相应的私钥进行绑定来增强安全性。Active Directory 证书服务还包括允许在各种可伸缩环境中管理证书注册及吊销的功能 Active Directory 证书服务所支持的应用领域包括安全/多用途 Internet 邮件扩展(S/MIME)、安全的无线网络、虚拟专用网络(VPN)、Internet 协议安全(IPsec)、加密文件系统(EFS)、智能卡登录、安全套接字层/传输层安全(SSL/TLS)以及数字签名
Active Directory 域服务	Active Directory 域服务(AD DS)存储有关网络上的用户、计算机和其他设备的信息。AD DS 帮助管理员安全地管理此信息并促使在用户之间实现资源共享和协作。此外，为了安装启用目录的应用程序(如 Microsoft Exchange Server)并应用其他 Windows Server 技术(如“组策略”)，还需要在网络上安装 AD DS
Active Directory 联合身份验证服务	Active Directory 联合身份验证服务(AD FS)提供了单一登录(SSO)技术，可使用单一用户账户在多个 Web 应用程序上对用户进行身份验证。AD FS 通过以下方式完成此操作：在伙伴组织之间以数字声明的形式安全地联合或共享用户标识和访问权限
Active Directory 轻型目录服务	对于其应用程序需要用目录来存储应用程序数据的组织而言，可以使用 Active Directory 轻型目录服务(AD LDS)作为数据存储方式。AD LDS 作为非操作系统服务运行，因此，并不需要在域控制器上对其进行部署。作为非操作系统服务运行，可允许多个 AD LDS 实例在单台服务器上同时运行，并且可针对每个实例单独进行配置，从而服务于多个应用程序
Active Directory 权限管理服务	Active Directory 权限管理服务(AD RMS)是一项信息保护技术，可与启用了 AD RMS 的应用程序协同工作，帮助保护数字信息免遭未经授权的使用。内容所有者可以准确地定义收件人可以使用信息的方式，例如，谁能打开、修改、打印、转发和/或对信息执行其他操作。组织可以创建自定义的使用权限模板，如“机密-只读”，此模板可直接应用到诸如财务报表、产品说明、客户数据及电子邮件之类的信息
应用程序服务器	应用程序服务器提供了完整的解决方案，用于托管和管理高性能分布式业务应用程序。诸如 .NET Framework、Web 服务器支持、消息队列、COM+、Windows Communication Foundation 和故障转移群集之类的集成服务有助于在整个应用程序生命周期(从设计与开发直到部署与操作)中提高工作效率

续表

角色名称	描　述
动态主机配置协议(DHCP)服务器	动态主机配置协议允许服务器将 IP 地址分配给作为 DHCP 客户端启用的计算机和其他设备，也允许服务器租用 IP 地址。通过在网络上部署 DHCP 服务器，可为计算机及其他基于 TCP/IP 的网络设备自动提供有效的 IP 地址及这些设备所需的其他配置参数(称为 DHCP 选项)，这些参数允许它们连接到其他网络资源，如 DNS 服务器、WINS 服务器及路由器
DNS 服务器	域名系统(DNS)提供了一种将名称与 Internet 数字地址相关联的标准方法。这样，用户就可以使用容易记住的名称代替一长串数字来访问网络计算机。在 Windows 上，可以将 Windows DNS 服务和动态主机配置协议(DHCP)服务集成在一起，这样在将计算机添加到网络时，就无须添加 DNS 记录
传真服务器	传真服务器，可发送和接收传真，并允许管理这台计算机或网络上的传真资源，例如作业、设置、报告以及传真设备等
文件服务	文件服务，提供了实现存储管理、文件复制、分布式命名空间管理、快速文件搜索和简化的客户端文件访问等技术
网络策略和访问服务	网络策略和访问服务提供了多种方法，可向用户提供本地和远程网络连接及连接网络段，并允许网络管理员集中管理网络访问和客户端健康策略。使用网络访问服务，可以部署 VPN 服务器、拨号服务器、路由器和受 802.11 保护的无线访问。还可以部署 RADIUS 服务器和代理，并使用连接管理器管理工具包来创建允许客户端计算机连接到网络的远程访问配置文件
打印服务	可以使用打印服务来管理打印服务器和打印机。打印服务器可通过集中打印机管理任务来减少管理工作负荷
终端服务	终端服务，所提供的技术允许用户从任何计算设备访问安装在终端服务器上的基于 Windows 的程序，或访问 Windows 桌面本身。用户可连接到终端服务器来运行程序并使用该服务器上的网络资源
通用描述、发现和集成(UDDI)服务	UDDI 服务提供了通用描述、发现和集成(UDDI)功能，用于在组织的 Intranet 内、Intranet 或 Internet 上的业务伙伴之间共享有关 Web 服务的信息。UDDI 服务通过更可靠和可管理的应用程序提高开发人员和 IT 专业人员的工作效率。使用 UDDI 服务，可以促进现有开发成果的重复使用，从而避免重复劳动
Web 服务器(IIS)	使用 Web 服务器(IIS)可以共享 Internet、Intranet 或 Extranet 上的信息。它是统一的 Web 平台，集成了 IIS 7.0、ASP.NET 和 Windows Communication Foundation。IIS 7.0 还具有安全性增强、诊断简化和委派管理等特点
Windows 部署服务	可以使用 Windows 部署服务在带有预启动执行环境(PXE)启动 ROM 的计算机上远程安装并配置 Microsoft® Windows 操作系统。WdsMgmt Microsoft 管理控制台(MMC)管理单元可管理 Windows 部署服务的各个方面，实施该管理单元将减少管理开销。Windows 部署服务还可以为最终用户提供与使用 Windows 安装程序相一致的体验
Hyper-V™	Hyper-V 提供服务，可以使用这些服务创建和管理虚拟机及其资源。每个虚拟机都是一个在独立执行环境中运行的虚拟化计算机系统。这允许用户同时运行多个操作系统

3.1.2　角色服务

对于管理员来说，可以一目了然地看到服务器上安装的所有角色和角色的运行情况，而且所有的配置都在一个界面中，管理起来相当方便，比起 Windows Server 2003 确实强大了许多。在此之前一直需要手动将不同的管理工具添加到一个 MMC 控制台中，现在 Windows Server 2008 已经为用户整合好了，而且从这里获得的信息量也比以前多很多。

角色服务是提供角色功能的软件程序。安装角色时，可以选择角色将为企业中的其他用户和计算机提供的角色服务。一些角色(例如 DNS 服务器)只有一个功能，因此没有可用的角色服务。其他角色(比如终端服务)可以安装多个角色服务，这取决于企业的远程计算需要。

可以将角色视为对密切相关的互补角色服务的分组，在大多数情况下，安装角色意味着安装该角色的一个或多个角色服务。

3.1.3　功能

功能是一些软件程序，这些程序虽然不直接构成角色，但可以支持或增强一个或多个角色的功能，或增强整个服务器的功能，而不管安装了哪些角色。例如，“故障转移群集”功能增强其他角色(比如文件服务和 DHCP 服务器)的功能，方法是使它们可以针对已增加的冗余和改进的性能加入服务器群集。另一个功能“Telnet 客户端”允许通过网络连接与 Telnet 服务器远程通信，从而全面增强服务器的通信选项，图 3-3 显示了 Windows Server 2008 的所有功能。表 3-2 为功能描述。



图 3-3　Windows Server 2008 的功能

表 3-2　功能描述

功　能	描　述
.NET Framework 3.0	.NET Framework 3.0 将 .NET Framework 2.0 API 的强大功能与新技术组合在一起，以构建功能强大的应用程序，这些应用程序提供引人注目的用户界面，保护客户的个人标识信息，支持无缝、安全的通信，并提供为一系列业务过程建模的功能
BitLocker 驱动器加密	BitLocker 驱动器加密通过加密整个卷并检查早期启动组件的完整性，来帮助保护已丢失、已盗或解除授权不当的计算机上的数据。只有成功验证这些组件且已加密的驱动器位于原来的计算机时，数据才会被解密。完整性检查需要兼容的受信任的平台模块(TPM)

续表

功　能	描　述
BITS 服务器扩展	后台智能传送服务(BITS)服务器扩展允许服务器接收客户端使用 BITS 上载的文件。BITS 允许客户端计算机在前台或后台异步传送文件，保持对其他网络应用程序的响应，并在网络出现故障和计算机重新启动后恢复文件传送
连接管理器管理工具包	连接管理器管理工具包(CMAK)可生成连接管理器配置文件
桌面体验	桌面体验包括 Windows Vista® 的功能，如 Windows Media Player、桌面主题和照片管理。桌面体验在默认情况下不会启用任何 Windows Vista 功能，必须手动启用它们
组策略管理	借助组策略管理，可以更方便地了解、部署、管理组策略的实施并解决疑难问题。其标准工具是组策略管理控制台(GPMC)，这是一种脚本化的 Microsoft 管理控制台(MMC)管理单元，提供了用于在企业中管理组策略的单一管理工具
Internet 打印客户端	Internet 打印客户端允许使用 HTTP 连接到 Web 打印服务器上的打印机，并使用这些打印机。Internet 打印实现了不同域或网络中的用户与打印机之间的连接。使用示例包括在远程办公地点出差的员工，或在备有 Wi-Fi 访问权限的咖啡店休息的员工
Internet 存储名称服务器	Internet 存储名称服务器(iSNS)为 Internet 小型计算机系统接口(iSCSI)存储区域网络提供了发现服务。iSNS 可以处理注册请求、注销请求，以及来自 iSNS 客户端的查询
LPR 端口监视器	Line Printer Remote(LPR)端口监视器允许有权访问基于 UNIX 的计算机用户在与计算机连接的设备上进行打印
消息队列	消息队列提供安全可靠的消息传递、高效路由和安全性，以及在应用程序间进行基于优先级的消息传递。消息队列还适用于在下列情况下的应用程序之间进行消息传递：这些应用程序在不同的操作系统上运行，使用不同的网络设施，暂时脱机，或在不同的时间运行
多路径 I/O	多路径 I/O(MPIO)与 Microsoft 设备特定模块(DSM)或第三方 DSM 一起，为 Microsoft Windows 上的存储设备使用多个数据路径提供支持
对等名称解析协议	对等名称解析协议(PNRP)允许应用程序通过用户的计算机进行注册和解析名称，以使其他计算机可与这些应用程序进行通信
优质 Windows 音频视频体验	优质 Windows 音频视频体验(qWave)是 Internet 协议家庭网络上音频和视频(AV)流应用程序的网络平台。通过确保 AV 应用程序的网络服务质量，qWave 增强了 AV 流的性能和可靠性。它提供了许可控制、运行时监控和强制执行、应用程序反馈以及通信优先级等机制。在 Windows Server 平台上，qWave 只提供流量率和优先级服务
远程协助	远程协助能让你(或支持人员)向具有计算机问题或疑问的用户提供协助。远程协助允许你查看和共享用户桌面的控制权，以解答疑问和修复问题。同时，用户还可以向朋友或同事寻求帮助
远程服务器管理工具	使用远程服务器管理工具，可以从运行 Windows Server 2008 的计算机上对 Windows Server 2003 和 Windows Server 2008 进行远程管理，用户可以在远程计算机上运行一些角色、角色服务和功能管理工具
可移动存储管理器	可移动存储管理器(RSM)对可移动介质进行管理和编录，并对自动化可移动介质设备进行操作
RPC Over HTTP 代理	RPC Over HTTP 代理由通过超文本传输协议(HTTP)接收远程过程调用(RPC)的对象使用。客户端可借助此代理发现这些对象，即使这些对象在服务器之间移动，或者即使它们存在于网络的离散区域中(通常出于安全原因)
NFS 服务	网络文件系统(NFS)服务是可作为分布式文件系统的协议，可允许计算机轻松地通过网络访问文件，就像在本地磁盘上访问它们一样。仅在 Windows Server 2008 for Itanium-based Systems 中安装此功能；在其他版本的 Windows Server 2008 中，NFS 服务将作为文件服务角色的角色服务

续表

功 能	描 述
SMTP 服务器	SMTP 服务器支持在电子邮件系统之间传送电子邮件
SAN 存储管理器	存储区域网络(SAN)存储管理器可帮助在 SAN 中支持虚拟磁盘服务(VDS)的光纤通道子系统和 iSCSI 磁盘驱动器子系统上创建和管理逻辑单元号(LUN)
简单 TCP/IP 服务	简单 TCP/IP 服务支持以下 TCP/IP 服务：Character Generator、Daytime、Discard、Echo 以及 Quote of the Day。简单 TCP/IP 服务用于向后兼容，只在需要时进行安装
SNMP 服务	简单网络管理协议(SNMP)是 Internet 标准协议，用于在管理控制台应用程序(如 HP Openview、Novell NMS、IBM NetView 或 Sun Net Manager)和托管实体之间交换管理信息。托管实体可以包括主机、路由器、桥和集线器
基于 UNIX 应用程序的子系统	将基于 UNIX 应用程序的子系统(SUA)和 Microsoft 网站可供下载的支持实用程序包一起使用，就能够运行基于 UNIX 的程序，并能在 Windows 环境中编译并运行自定义的基于 UNIX 的应用程序
Telnet 客户端	Telnet 客户端可使用 Telnet 协议连接到远程 Telnet 服务器并运行该服务器上的应用程序
Telnet 服务器	Telnet 服务器允许远程用户(包括那些运行基于 UNIX 的操作系统的用户)执行命令行管理任务并通过使用 Telnet 客户端来运行程序
普通文件传输协议(TFTP) 客户端	普通文件传输协议(TFTP)客户端用于从远程 TFTP 服务器中读取文件，或将文件写入远程 TFTP 服务器。TFTP 主要由嵌入式设备或系统使用，它们可在启动过程中从 TFTP 服务器检索固件、配置信息或系统映像
故障转移群集	故障转移群集允许多台服务器一起工作，以实现服务及应用程序的高可用性。故障转移群集常用于文件和打印服务，以及数据库和邮件应用程序
网络负载平衡	网络负载平衡(NLB)使用 TCP/IP 网络协议在多台服务器中分配流量。当负载增加时，NLB 通过添加其他服务器来确保无状态应用程序(如运行 Internet 信息服务(IIS)的 Web 服务器)可以伸缩，此时 NLB 特别有用
Windows Server Backup	Windows Server Backup 允许对操作系统、应用程序和数据进行备份和恢复。可以将备份安排为每天运行一次或更频繁，并且可以保护整个服务器或特定的卷
Windows 系统资源管理器	Windows 系统资源管理器(WSRM)是 Windows Server 操作系统管理工具，可控制 CPU 和内存资源的分配方式。对资源分配进行管理可提高系统性能并减少应用程序、服务或进程因互相干扰而降低服务器效率和系统响应能力的风险
Windows Internet 名称服务 (WINS) 服务器	Windows Internet 名称服务(WINS)服务器提供分布式数据库，为网络上使用的计算机和组提供注册和查询 NetBIOS 动态映射名称的服务。WINS 将 NetBIOS 名称映射到 IP 地址，并可解决在路由环境中解析 NetBIOS 名称引起的问题
无线 LAN 服务	不管计算机是否具有无线适配器，无线 LAN (WLAN)服务都可配置并启动 WLAN 自动配置服务。WLAN 自动配置可枚举无线适配器，并可管理无线连接和无线配置文件，这些配置文件包含用于配置无线客户端使其连接到无线网络所需的设置
Windows Internal Database	Windows Internal Database 是仅可供 Windows 角色和功能(如 UDDI 服务、Active Directory 权限管理服务(AD RMS)、Windows 服务器更新服务和 Windows 系统资源管理器)使用的关系型数据存储
Windows PowerShell	Windows PowerShell 是一种命令行 Shell 和脚本语言，可帮助 IT 专业人员提高工作效率。它提供了新的侧重于管理员的脚本语言和 130 多种标准命令行工具，可使系统管理变得更轻松并可加速实现自动化功能

续表

功　能	描　述
Windows 进程激活服务	Windows 进程激活服务(WAS)通过删除对 HTTP 的依赖关系，可统一 IIS 进程模型。通过使用非 HTTP 协议，以前只可用于 HTTP 应用程序的 IIS 的所有功能现在都可用于运行 Windows Communication Foundation (WCF)服务的应用程序。IIS 7.0 还使用 WAS 通过 HTTP 实现基于消息的激活

3.2 服务器管理器

服务器管理器是扩展的 Microsoft 管理控制台(MMC)，允许查看和管理影响服务器工作效率的几乎所有信息和工具。

服务器管理器允许管理员使用单个工具就可完成以下任务，从而使服务器管理更高效。

- 查看和更改服务器上已安装的服务器角色及功能。
- 执行与服务器的运行生命周期相关联的管理任务，如启动或停止服务以及管理本地用户账户。
- 执行与服务器上已安装角色的运行生命周期相关联的管理任务。
- 确定服务器状态，识别关键事件，分析并解决配置问题和故障。

服务器管理器中的功能

如图 3-4 所示，服务器管理器包括以下功能。

- 初始配置任务。完成安装 Windows Server® 2008 之后，在企业中部署新服务之前，需要一些配置来标识计算机，使用户的网络中的其他计算资源识别该计算机，保护计算机，并通过添加服务器角色和功能自定义计算机。
- 可以通过在“初始配置任务”窗口中使用命令来完成这些任务，此窗口在操作系统安装完成之后会立即打开。
- 在服务器上安装或删除角色、角色服务和功能的简单、易用的向导。管理员不再需要使用“添加或删除 Windows 组件”安装或配置服务器角色，也不必担心在安装或删除角色或功能期间丢失重要的软件程序。可以通过使用“服务器管理器”向导在单个会话中安装或删除多个角色、角色服务或功能。简单并且有提示信息的向导消除了猜测。

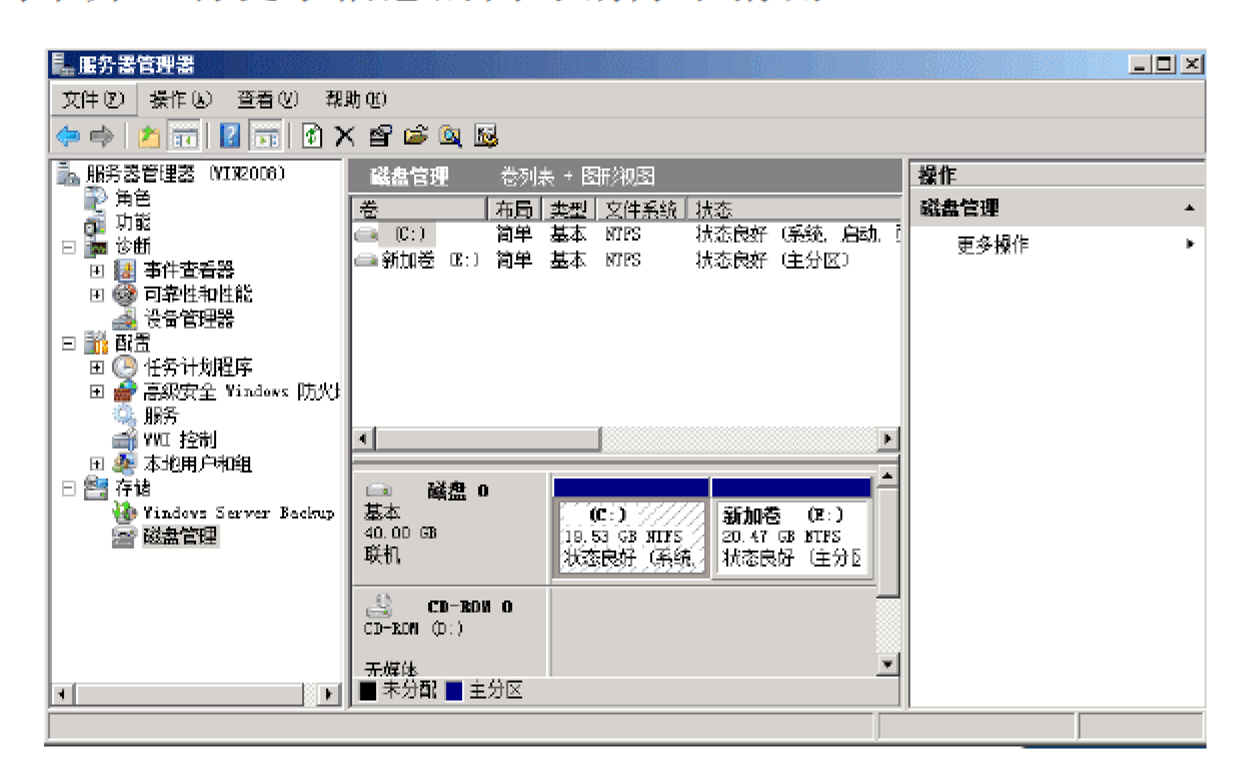


图 3-4　“服务器管理器”窗口

“服务器管理器”中的可用向导如下。

- 添加角色向导。
- 删除角色向导。
- 添加角色服务向导。
- 删除角色服务向导。
- 添加功能向导。
- 删除功能向导。

每个已安装服务器角色的主页，即使在服务器上安装了多个服务器角色，管理员也可以使用“服务器管理器”执行针对所有这些角色的管理任务。

“服务器管理器”主窗口中可展开的“功能”部分将显示已安装的功能，并提供可用于安装和删除功能的命令。“服务器管理器”中的“功能”主页显示有关已安装功能的详细信息，其中包括对已安装功能的描述。

“服务器管理器”主窗口中可展开的“服务器摘要”部分。有关本地计算机、其身份、操作系统、网络连接和事件日志的信息可在一个方便的位置获得。“安全信息”区域显示是否在服务器上启用了 Windows 防火墙或 Windows 更新，并显示服务器检查更新的最近时间。

通过使用“服务器管理器”命令行实现的无人参与的角色、角色服务或功能安装。可以通过使用单个命令实例或通过使用 XML 答案文件来安装或删除角色、角色服务和功能。有关“服务器管理器”命令行的详细信息，可参阅“服务器管理器”的帮助。

3.3 实战 1：添加功能

任务描述

能够给服务器添加需要的功能，了解功能在服务器上的作用。

实战环境

- Windows Server 2008 企业版操作系统。
- 能够连接到 Internet。

实战目标

- 能够学会给服务器安装“Telnet 客户端”。
- 使用 telnet 命令测试是否能够访问服务器的某个端口。
- 能够给服务器安装“桌面体验”功能。
- 体会功能在服务器上的作用。

任务：在服务器上安装功能

以下步骤将会给服务器安装 Telnet 客户端和桌面体验，然后使用 telnet 命令测试能否打开远程服务器的某个端口，更改 Windows 主题为 Windows Vista 界面。

桌面体验功能是 Windows Server 2008 操作系统中的一项新功能。桌面体验包括 Windows Vista 操作系统中提供的多种应用程序和功能。如果将 Windows Server 2008 用作主要操作系统，则可能希望将其中某些 Windows Vista 功能用于日常使用。

什么是桌面体验功能

桌面体验功能包括下列 Windows Vista 组件和功能。

- Windows 日历。
- Windows Mail。
- Windows Media Player。
- Windows Aero(TM) 和其他桌面主题。
- Windows 视频(AVI 支持)。
- Windows 照片库。
- Windows SideShow(TM)。
- Windows Defender。
- 磁盘清理。
- 同步中心。
- 录音机。
- 字符映射。

以管理员的身份登录服务器，打开“服务器管理器”窗口。

① 如图 3-5 所示，选中“功能”选项，单击“添加功能”按钮。

② 如图 3-6 所示，在选择功能界面中，选中“Telnet 客户端”和“桌面体验”选项。

③ 单击“下一步”按钮，完成安装，重启系统。

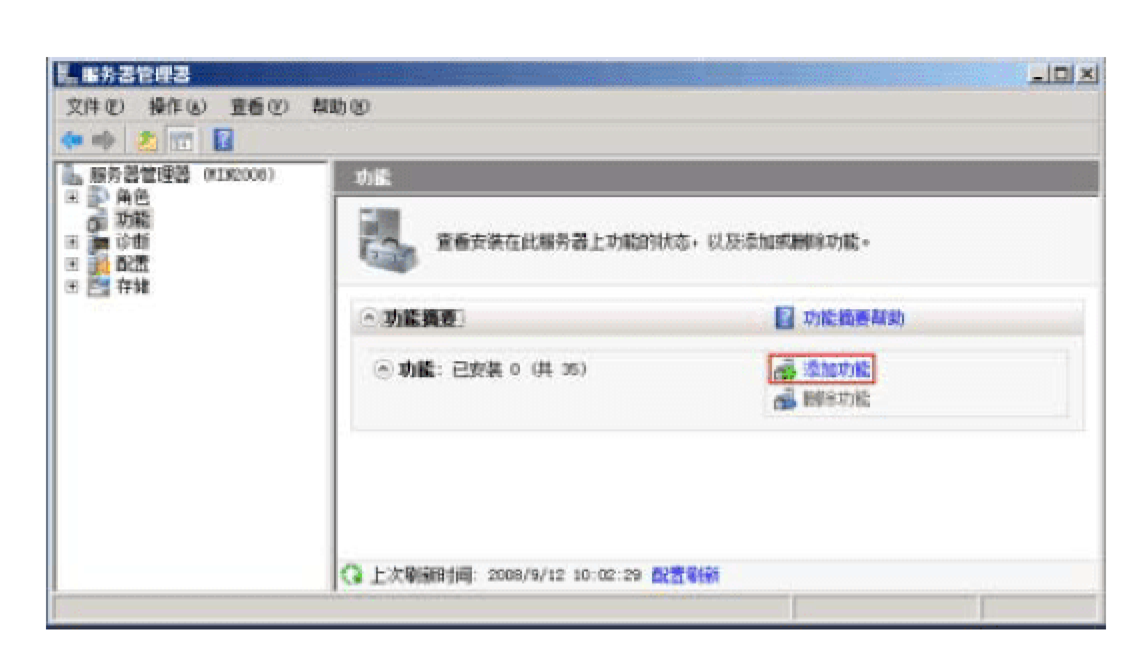


图 3-5 添加功能

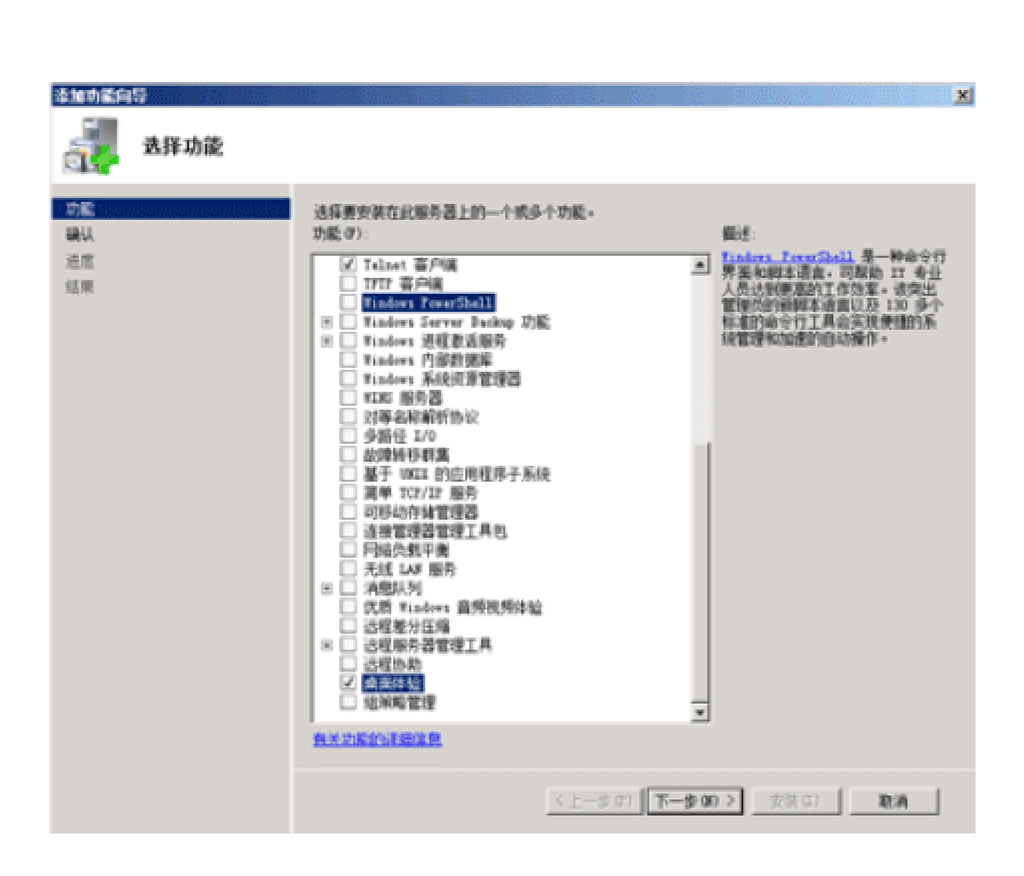


图 3-6 选择功能

④ 再次以管理员身份登录操作系统，打开“服务器管理”窗口，选择“配置”→“服务”命令，如图 3-7 所示，双击“Themes”服务。

⑤ 将其启动类型改为“自动”，单击“应用”按钮，单击“启动”按钮。

⑥ 右击桌面空白处，在弹出的快捷菜单中选择“个性化”命令，打开“主题设置”对话框，单击“主题”标签，如图 3-8 所示。可以选择 Windows Vista，单击“确定”按钮。此时，会发现 Windows Server 2008 界面变成了 Vista 风格。

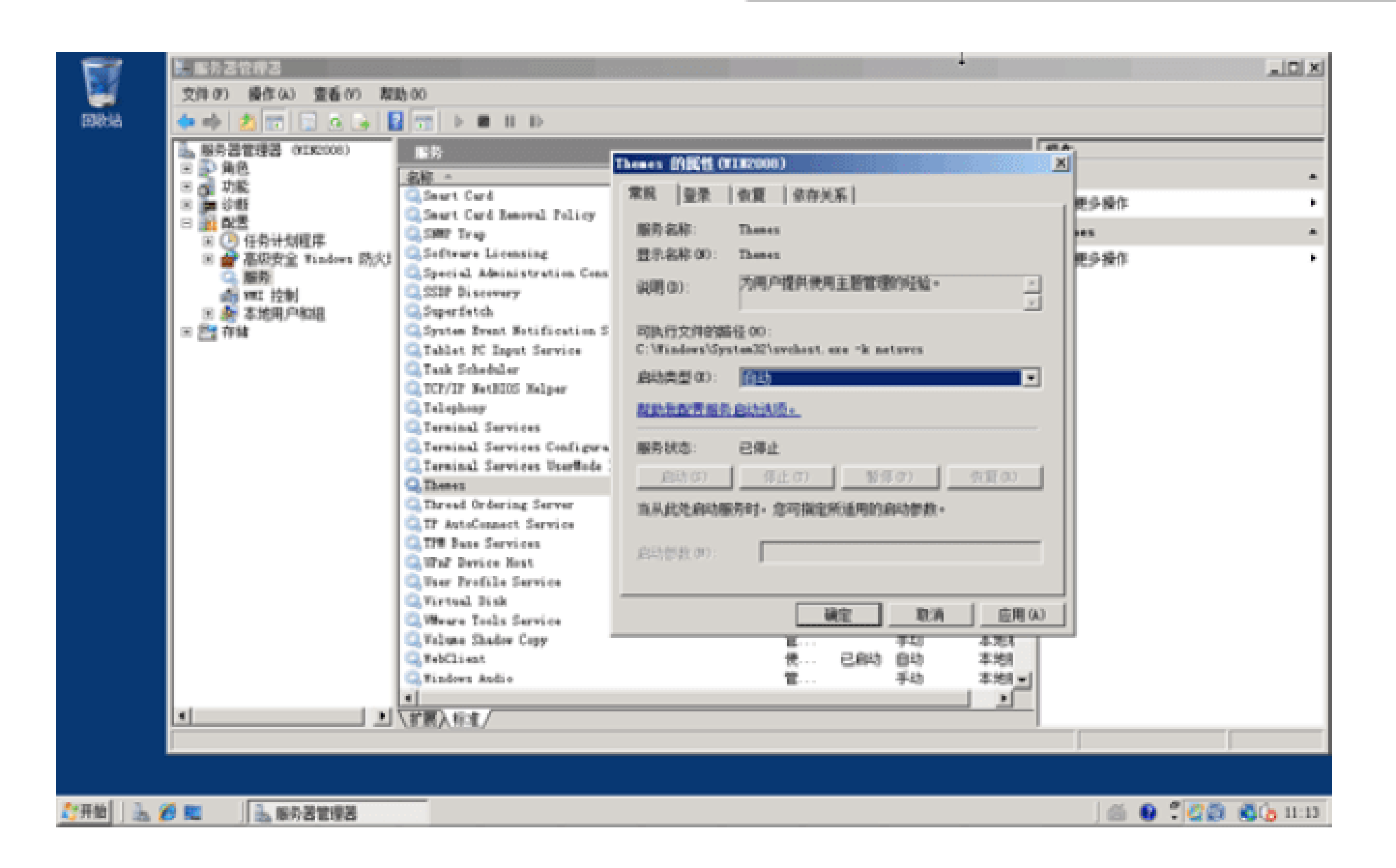


图 3-7　更改 Themes 服务启动类型

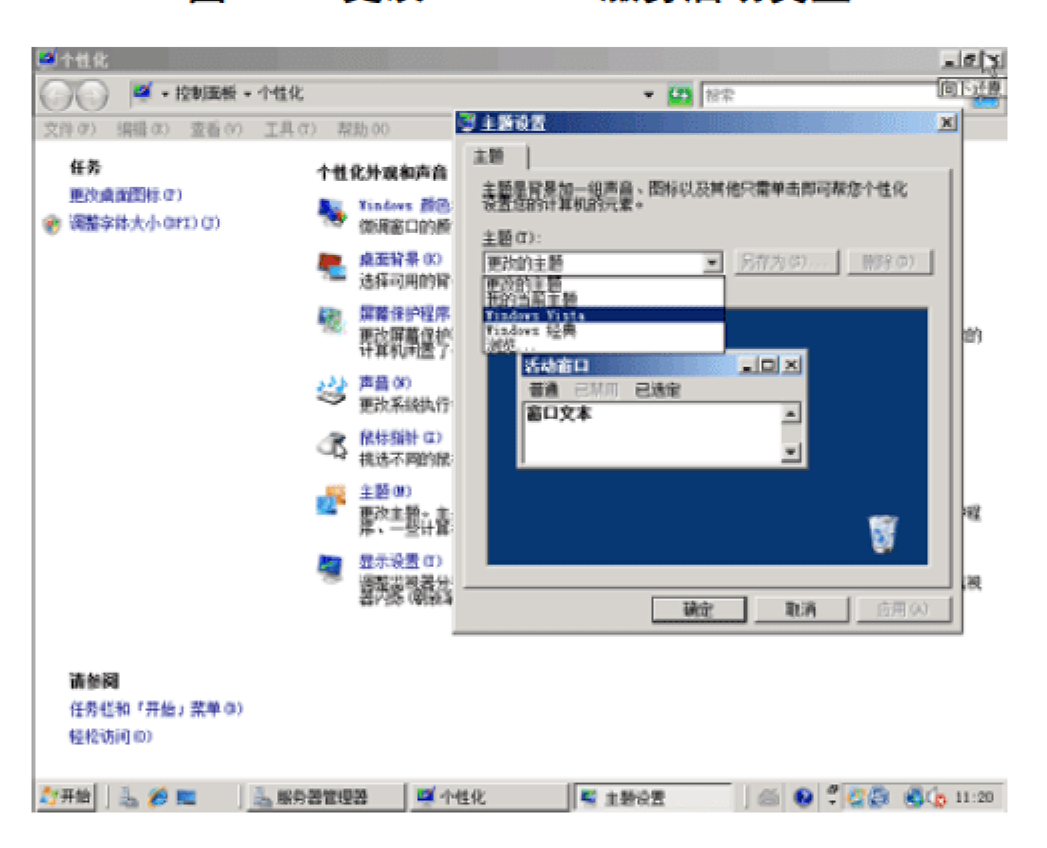


图 3-8　更改桌面主题

⑦ 选择“开始”→“运行”命令，在打开的“运行”对话框中输入 cmd，打开命令行界面。

⑧ 输入 telnet www.inhe.net 80，测试是否能够打开银河网站的 80 端口，如图 3-9 所示。

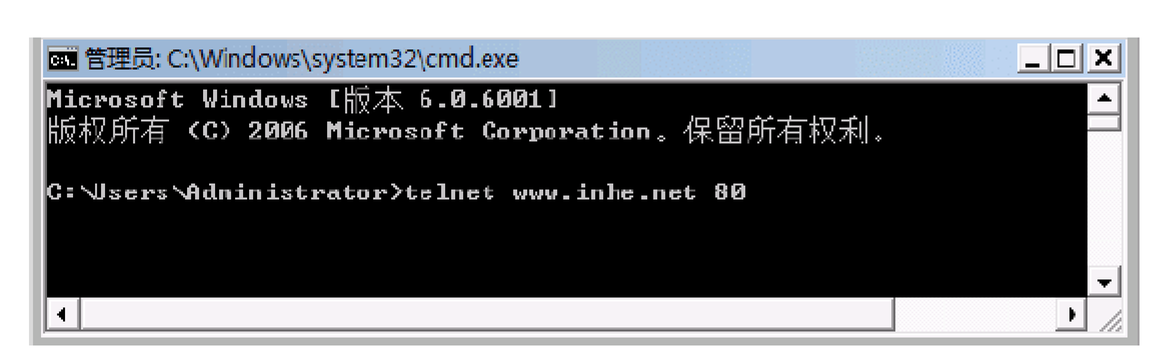


图 3-9　使用 telnet 测试能否访问服务器的某个端口

⑨ 如果出现如图 3-10 所示的窗口，则表示能够打开银河网站的 80 端口。注意，别关掉这个窗口。

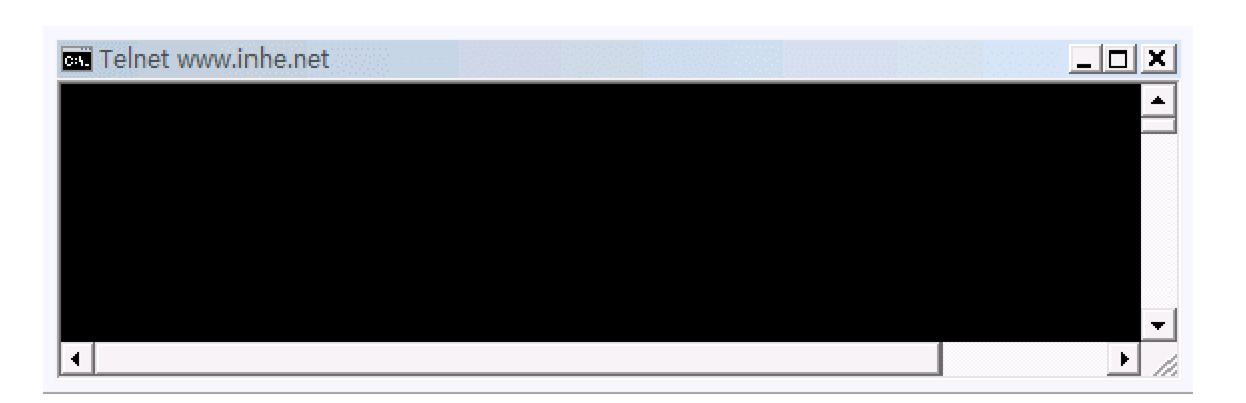


图 3-10　Telnet 成功

⑩ 再打开一个命令行窗口，输入 netstat –n，可以看到 Telnet 建立的会话，如图 3-11 所示。



图 3-11 查看到的会话

⑪ 如果出现如图 3-12 所示的窗口，则表示不能打开银河网站的 80 端口。这种情况下用 IE 浏览器也不能访问该网站。



图 3-12 打开端口失败

3.4 配置和管理硬件

1. 什么是驱动程序

驱动程序是一种允许计算机与硬件或设备之间进行通信的软件。如果没有驱动程序软件，连接的硬件(例如，视频卡或打印机)将无法正常工作。

多数情况下，Windows 附带驱动程序软件，或者可以通过转到“控制面板”中的 Windows Update 并检查是否有更新来查找驱动程序软件。如果 Windows 没有所需的驱动程序，则可以在要使用的硬件或设备附带的光盘中或者制造商的网站找到该驱动程序。

2. 什么是签名的驱动程序

签名的驱动程序是一种包含数字签名的设备驱动程序软件。数字签名是一种电子安全性标记，它可以指明软件的发行者，以及是否有人已更改驱动程序软件程序包的原有内容。如果驱动程序已由使用证书颁发机构验证其身份的发行者签名，则可以确信驱动程序软件实际来自该发布者并且没有被更改。

如果驱动程序软件没有签名，未由使用证书颁发机构验证其身份的发布者签名，或者自发行以来已进行了更改，则 Windows 将通过以下其中一条消息警告用户。

- 错误！超链接引用无效。
  该驱动程序软件没有数字签名，或者它的数字签名没有经过证书颁发机构的验证。如果用户通过原有制造商的光盘或通过系统管理员获取该驱动程序软件，则应只安装该驱动程序软件。
- 该驱动程序软件已被更改。
  该驱动程序软件由已验证的发行者进行数字签名之后已被更改。该程序包可能已被更改为包含可能损害计算机或盗取信息的恶意软件。极少数情况下，合法发行者在驱动程序软件程序包已进行数字签名之后确实对其进行过更改。如果用户通过原有制造商的光盘获取已更改的驱动程序软件，

则应只安装该软件。

- Windows 无法安装该驱动程序软件。
  缺少有效数字签名的驱动程序软件，或者对其进行签名之后已被更改的驱动程序软件不能安装在基于 x64 版本的 Windows 上。因此，如果用户运行的是基于 x64 版本的 Windows，则只会看到此消息。

如果试图安装驱动程序软件时看到这些消息中的任何消息，则应访问设备制造商的支持网站，以获取有数字签名的设备驱动程序软件。

3.4.1 设备管理器的用途

设备管理器具有以下用途。

- 确定计算机上的硬件是否工作正常。
- 更改硬件配置设置。
- 标识为每个设备加载的设备驱动程序，并获取有关每个设备驱动程序的信息。
- 更改设备的高级设置和属性。安装更新的设备驱动程序。
- “启用”、“禁用”和“卸载”设备。
- 回滚到驱动程序的前一版本。
- 基于设备的类型、按设备与计算机的连接或按设备所使用的资源来查看设备。
- 显示或隐藏不必查看，但对高级疑难解答而言可能必需的隐藏设备。

通常将使用设备管理器来检查硬件的状态以及更新计算机上的设备驱动程序。完全了解计算机硬件的高级用户还可以使用设备管理器的诊断功能解决设备冲突和更改资源设置。

一般来说，不需要使用设备管理器更改资源设置，因为在硬件安装过程中系统会自动分配资源。

3.4.2 卸载设备的过程

1. 卸载即插即用设备

通常，不需要卸载即插即用设备，只需断开或拔出设备就可以使 Windows 不加载或不使用驱动程序。某些设备可能要求先关闭计算机。

2. 卸载非即插即用设备

卸载非即插即用设备通常包括以下两个步骤。

① 使用设备管理器卸载设备。

② 从计算机中移除该设备。

使用设备管理器卸载非即插即用设备。卸载设备后，必须从计算机中物理地断开或移除设备。例如，如果设备连接到计算机外侧的端口，则关闭计算机，断开设备与端口的连接，然后拔出设备的电源线。

3. 启用和禁用与安装和卸载

可以禁用即插即用设备，而无须卸载可能再次连接的设备(如调制解调器)。禁用设备时，设备虽然与计算机保持物理连接，但 Windows 会更新系统注册表，以使启动计算机时不加载设备的设备驱动程序。启

用设备时，驱动程序将再次可用。如果想使计算机拥有多种硬件配置，或者如果拥有在扩展坞中使用的便携式计算机，则禁用设备很有用。

3.4.3 卸载或重新安装设备

本主题所提供的过程可以用于卸载和重新安装硬件设备。

- 卸载设备。
- 重新安装即插即用设备。
- 重新安装非即插即用设备。

本地 Administrators 组的成员身份或同等身份，是完成此过程的最低要求。可在此主题的“其他考虑事项”中查看详细信息。

1. 卸载设备

通常，卸载即插即用设备不需要使用设备管理器，只需从计算机断开即插即用设备即可。但是，根据设备的类型，可能必须重新启动计算机。

卸载设备的步骤如下。

① 打开“设备管理器”。

② 双击要卸载设备的类型。

③ 右击所需的特定设备，然后在弹出的快捷菜单中选择“卸载”命令。也可以双击设备，然后在“驱动程序”选项卡中单击“卸载”按钮。

④ 如图 3-13 所示，如果还要从驱动程序存储区中删除设备驱动程序包，则在“确认设备删除”对话框中选中“删除此设备的驱动程序软件”复选框。

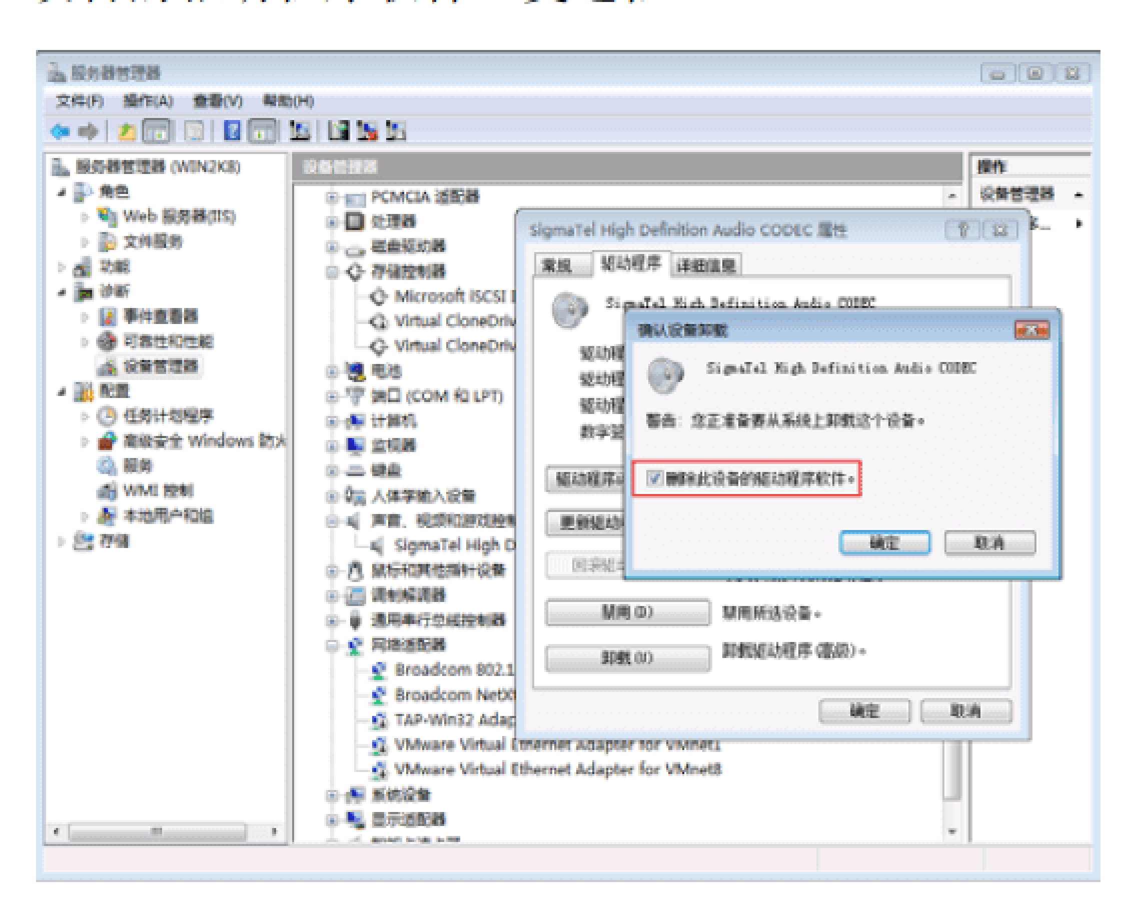


图 3-13 删除硬件驱动



提示：“删除此设备的驱动程序软件”选项将从驱动程序存储区中删除程序包。该选项不删除任何其他使用同一驱动程序的操作设备的当前所安装的驱动程序。如果从存储区中删除驱动程序，并将设备再次连接到计算机，则 Windows 必须在标准搜索位置中搜索驱动程序包的副本，包括可能会提示用户插入介质。

⑤　单击“确定”按钮，完成卸载过程。

⑥　卸载过程完成时，应从计算机中拔出设备。

如果系统提示重新启动计算机，则删除未完成，且设备可能继续运行，直到重新启动计算机为止。

2. 重新安装即插即用设备

只有在设备工作不正常或已完全停止工作时才需要重新安装设备。重新安装设备前，应尝试重新启动计算机并检查设备，以确定其是否正常运行。如果运行不正常，则应尝试重新安装该设备。

①　打开设备管理器。

②　按照前面过程中的说明执行操作以卸载设备。

3. 重新安装非即插即用设备

只有在设备工作不正常或已完全停止工作时才需要重新安装设备。重新安装设备前，应尝试重新启动计算机并检查设备，以确定其是否正常运行。如果运行不正常，则应尝试重新安装该设备。

①　打开设备管理器。

②　按照第一个过程中的说明执行操作以卸载设备。

③　右击细节窗格中顶部的节点。

④　在弹出的快捷菜单中选择“添加过时硬件”命令。

⑤　在“添加硬件向导”中，单击“下一步”按钮，然后按照屏幕上的说明执行操作。

3.4.4　修复或更新驱动程序

如果硬件设备未正常工作，或者安装的程序或游戏声明它需要比当前安装的驱动程序软件更新的驱动程序软件，则应检查 Windows Update 以获取更新的驱动程序软件。如果技术支持人员要求用户通过光盘或设备制造商的网站安装驱动程序软件，则还可以手动更新设备的驱动程序软件。

1. 使用 Windows Update 更新驱动程序软件

①　打开 Windows Update。如果系统提示用户输入管理员密码或进行确认，应输入密码或提供确认。

②　如图 3-14 所示，在左窗格中，单击“检查更新”选项。



图 3-14　检查更新

③　若要查看是否有更新的驱动程序软件可用，如图 3-15 所示，单击“查看可用更新”按钮。Windows Update 将列出计算机中已安装设备可用的所有更新的驱动程序软件。

④　如图 3-16 所示，如果更新可用，则单击要安装的驱动程序软件，然后单击“安装”按钮。如果系统提示输入管理员密码或进行确认，应输入密码或提供确认。



图 3-15　查看可用的更新

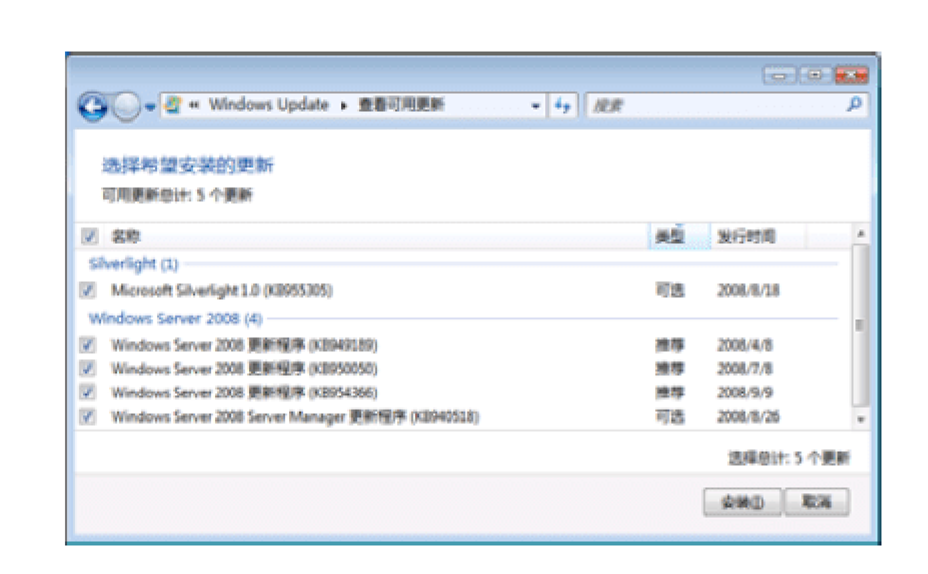


图 3-16　可用的更新

2. Windows Update 驱动程序设置

以下设置将会配置计算机连接新设备时，使用 Windows Update 自动检查驱动程序。

① 打开“服务器管理器”，如图 3-17 所示，单击“更改系统属性”按钮，在“系统属性”对话框中，单击“Windows Update 驱动程序设置”按钮。

② 如图 3-18 所示，选中“自动检查驱动程序”单选按钮，单击“确定”按钮。

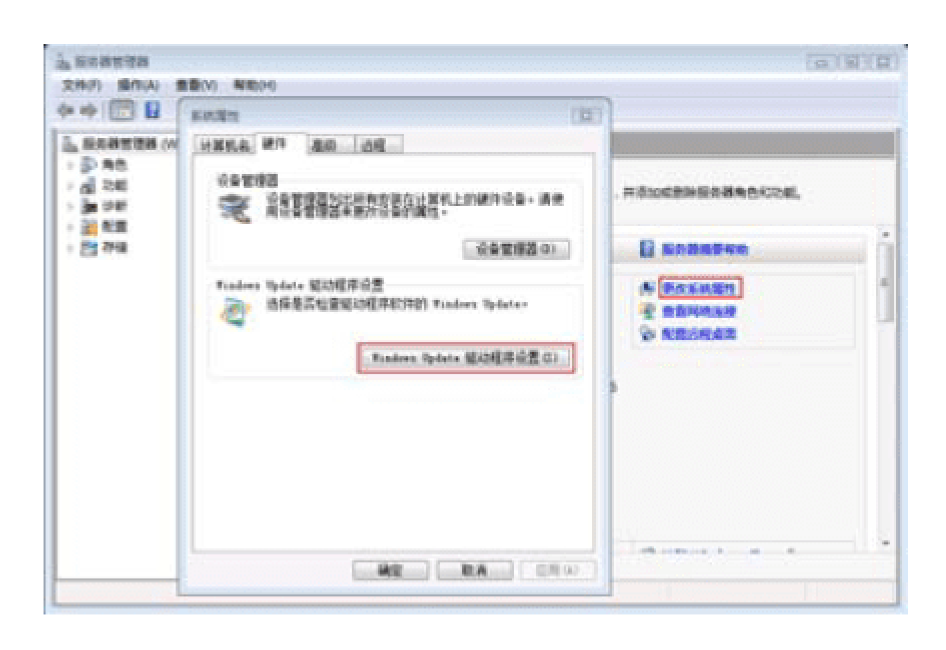


图 3-17　Windows Update 驱动程序设置

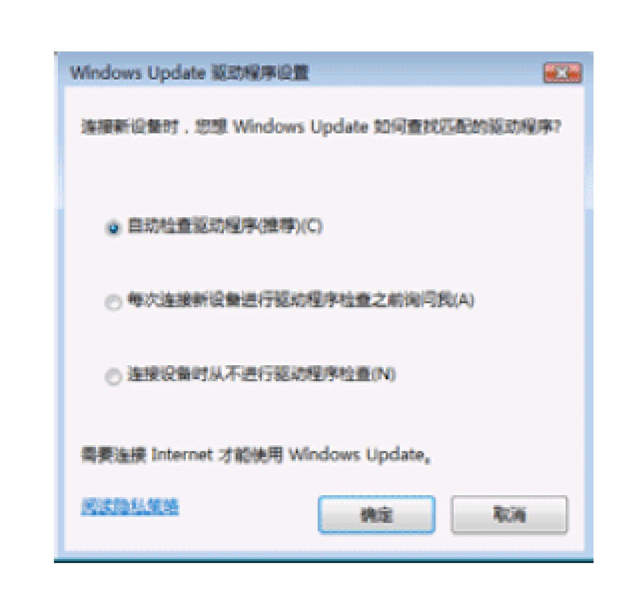


图 3-18　设置自动检查驱动程序

3. 手动更新驱动程序软件

必须以管理员身份进行登录，才能执行这些步骤。

① 打开设备管理器。如果系统提示输入管理员密码或进行确认，应输入密码或提供确认。

② 如图 3-19 所示，在设备管理器中，找到要更新的设备，然后双击该设备名称。

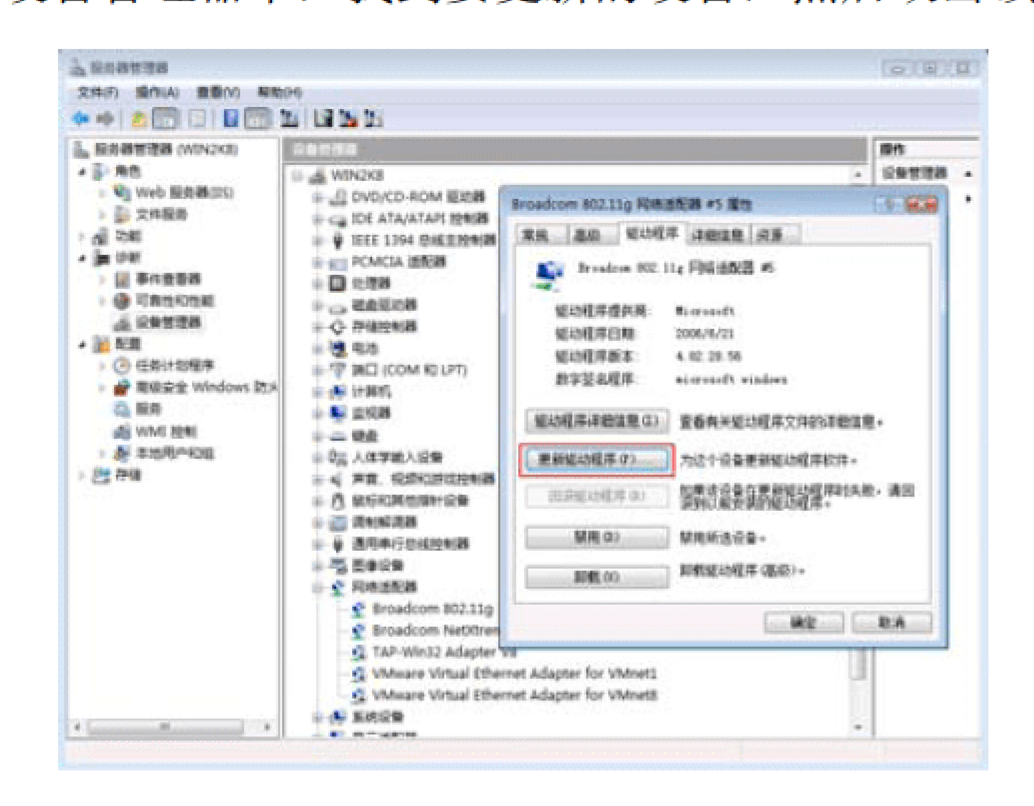


图 3-19　手动更新驱动程序

③　切换到“驱动程序”选项卡，然后单击“更新驱动程序”按钮即可。

3.4.5　将驱动程序还原到以前的版本

必须以管理员身份进行登录，才能执行这些步骤。

如果升级驱动程序软件之后，计算机或设备出现问题，可能希望将设备的驱动程序软件还原到以前的版本。

①　打开设备管理器。如果系统提示输入管理员密码或进行确认，应输入密码或提供确认。

②　双击包含设备驱动程序的类别，然后双击要还原到以前的驱动程序版本的设备名称。

③　切换到“驱动程序”选项卡，然后单击“回滚驱动程序”按钮，如图 3-20 所示。

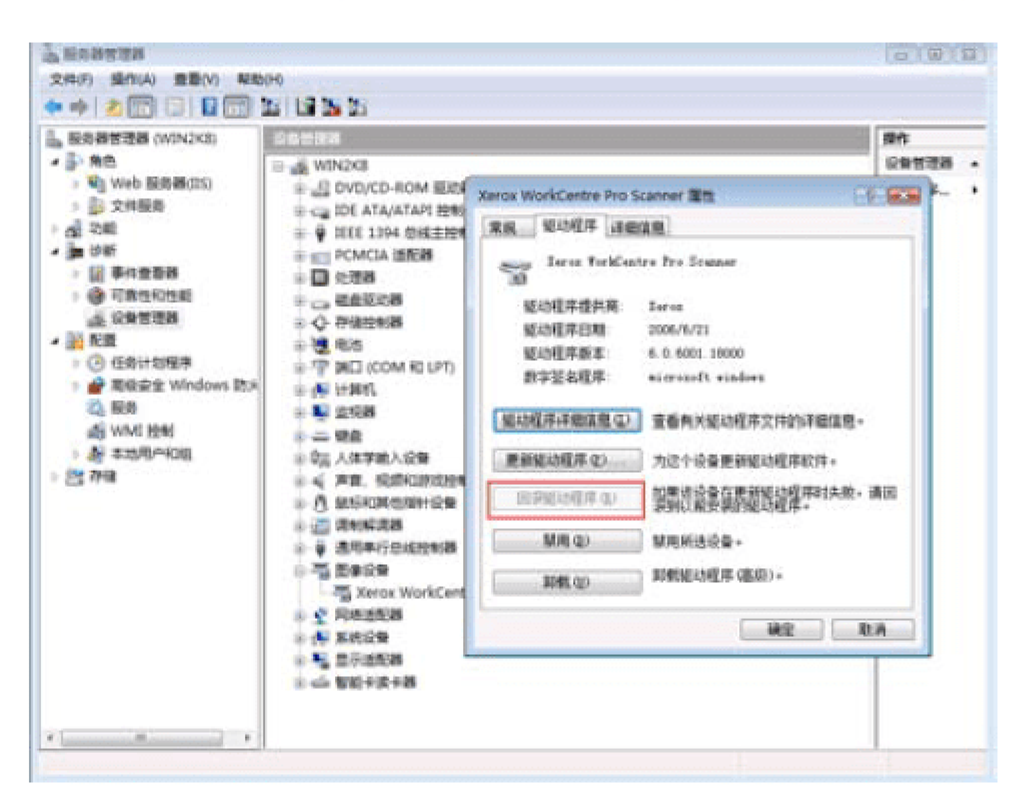


图 3-20　回滚驱动程序



注意：如果选定的设备没有安装以前版本的驱动程序软件，则“回滚驱动程序”按钮将不可用。

3.5　实战 2：配置用户和系统环境

任务描述

能够配置用户的桌面环境、开始菜单以适应用户的使用习惯，能够配置用户环境变量和系统变量。

实战环境

- Windows Server 2008 企业版操作系统。
- 能够连接到 Internet。

实战目标

- 设置桌面环境。
- 设置开始菜单。
- 配置用户环境变量和系统变量。
- 使用系统配置排除系统故障。

■ 配置文件夹选项。

3.5.1 任务 1：设置用户的桌面环境

将常用桌面图标显示在桌面上。

① 如图 3-21 所示，右击桌面，在弹出的快捷菜单中选择“个性化”命令。此时桌面上没有“计算机”、“回收站”、“控制面板”、“用户的文件”、“网络”等图标。

② 如图 3-22 所示，在“个性化”对话框中，单击“更改桌面图标”选项。在个性化设置对话框中，可以设置“Windows 颜色和外观”、“桌面背景”、“屏幕保护程序”、“声音”、“鼠标指针”、“主题”和“显示设置”。

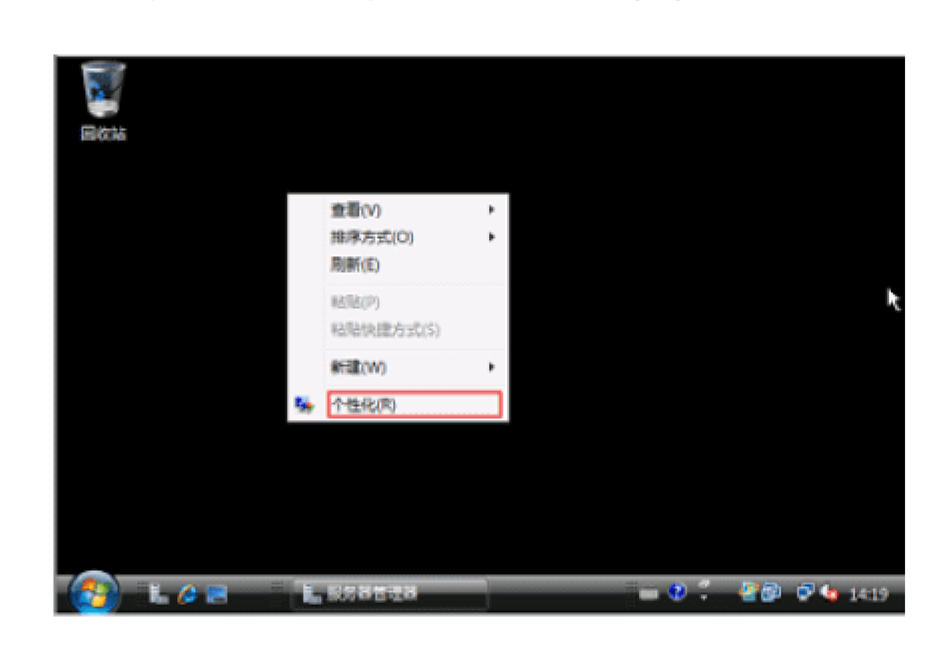


图 3-21　个性化桌面



图 3-22　更改桌面图标

③ 如图 3-23 所示，在“桌面图标设置”对话框中，分别选中“计算机”、“回收站”、“控制面板”、“用户的文件”、“网络”复选框，单击“确定”按钮。

④ 如图 3-24 所示，此时可以在桌面上看到这些图标。



图 3-23　选择桌面上显示的图标

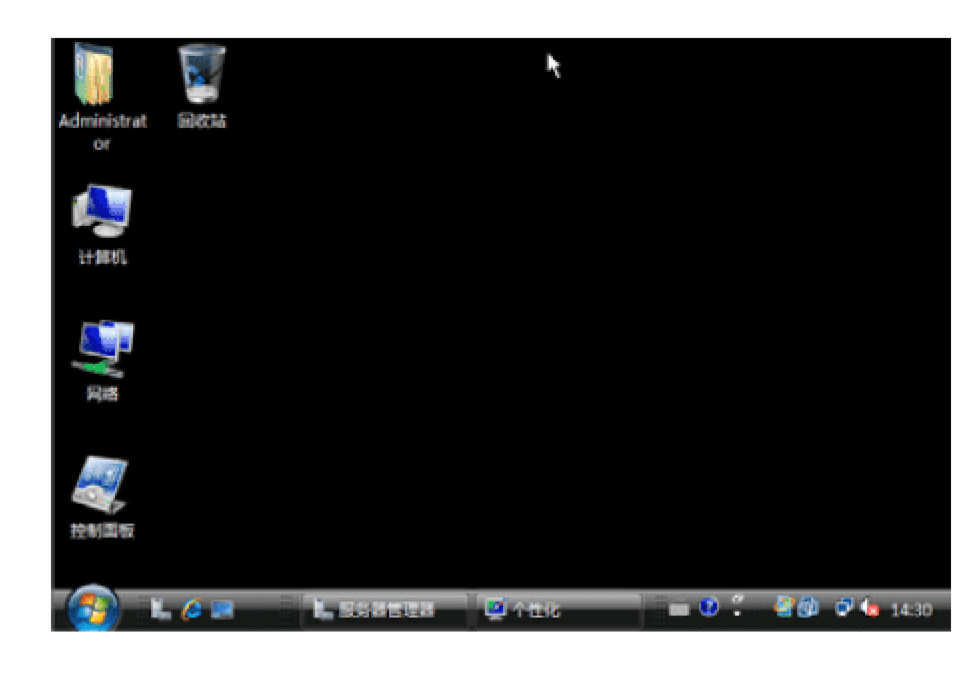


图 3-24　桌面上显示的图标

3.5.2 任务 2：自定义任务栏和开始菜单

将“开始”菜单改成经典模式，扩展控制面板和显示管理工具。

① 单击按钮，默认“开始”菜单如图 3-25 所示。如果不适合自己的使用习惯，则可将其改为传统的“开始”菜单。

② 如图 3-26 所示，右击任务栏和“开始”菜单，在弹出的快捷菜单中选择“属性”命令。



图 3-25　开始菜单



图 3-26　打开开始菜单属性

③　在“任务栏和「开始」菜单属性”对话框中，选中“传统「开始」菜单”单选按钮，如图 3-27 所示，单击“确定”按钮。

④　再次单击按钮，如图 3-28 所示，则将看到传统的“开始”菜单。



图 3-27　选中“传统「开始」菜单”单选按钮

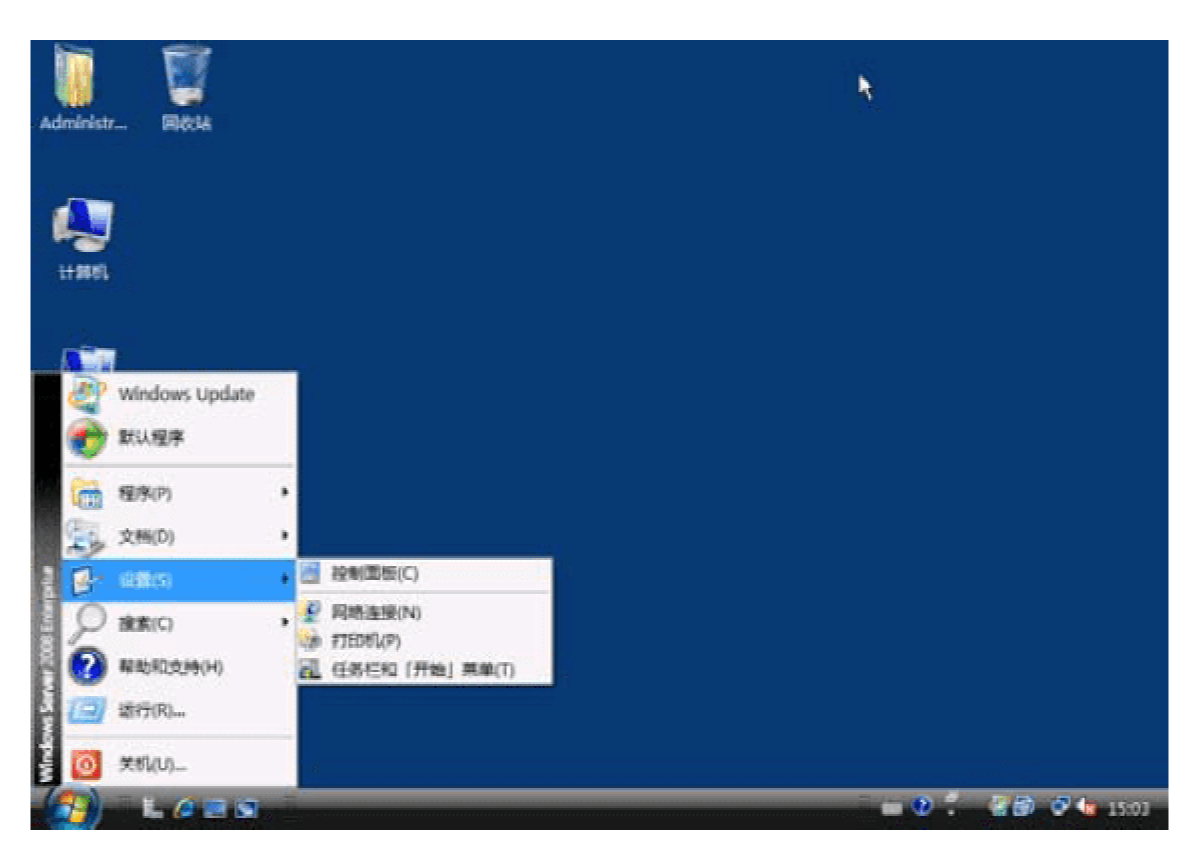


图 3-28　传统的“开始”菜单

⑤　如图 3-29 所示，在“任务栏和「开始」菜单属性”对话框中，单击“自定义”按钮。

⑥　如图 3-30 所示，选中“扩展控制面板”、“显示管理工具”复选框，单击“确定”按钮。

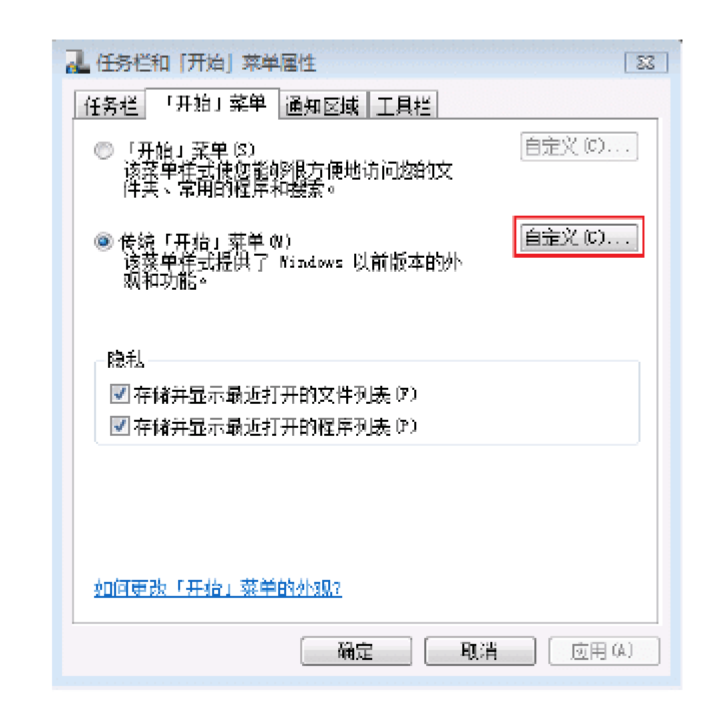


图 3-29　自定义开始菜单

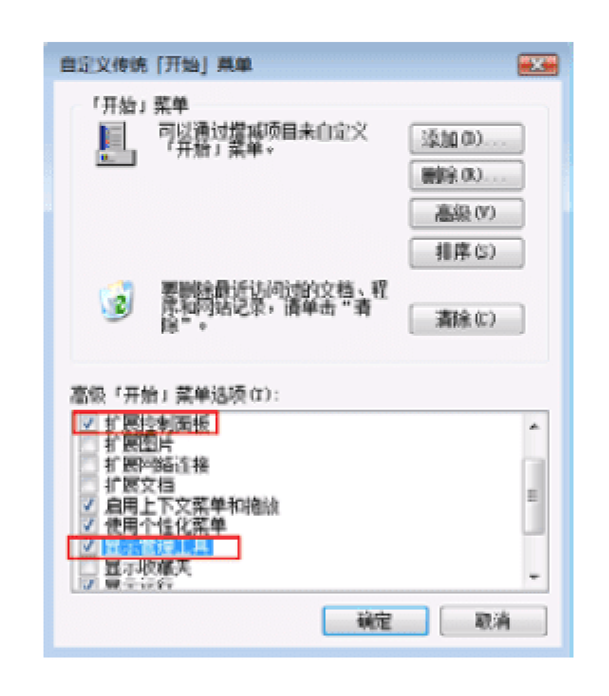


图 3-30　扩展控制面板和显示管理工具

⑦ 再次选择“开始”→“设置”→“控制面板”命令，如图 3-31 所示，可以看到任务面板中的内容显示出来了。

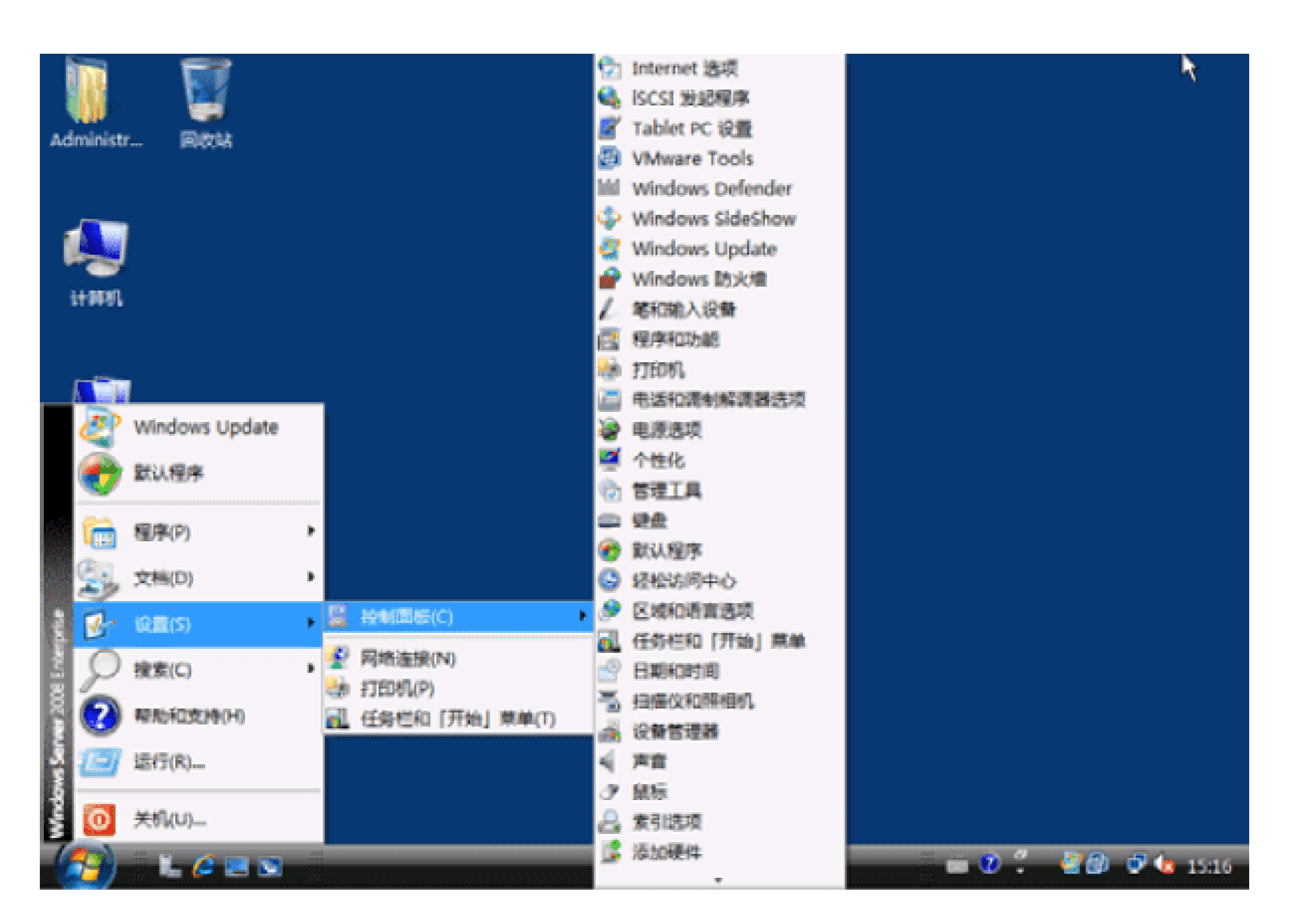


图 3-31　验证扩展的控制面板

3.5.3　任务 3：更改用户的环境变量和系统环境变量

对于特定的计算机来说，它的各个用户的环境变量各不相同，都是它们各自配置文件的组成部分。

- 系统环境变量应用于整个系统。
- 如果系统盘不够用了，则可以将当前用户的临时文件位置指定到其他分区。
- 如果将程序放到了 D 盘 app 文件夹下，欲在命令行任何路径下都能够运行时，自动搜索 D:\app 目录，则需要更改系统变量 Path 的值，添加 D:\app。

① 打开“服务器管理器”，单击“更改系统属性”按钮。

② 如图 3-32 所示，在出现的“系统属性”对话框中，单击“环境变量”按钮。

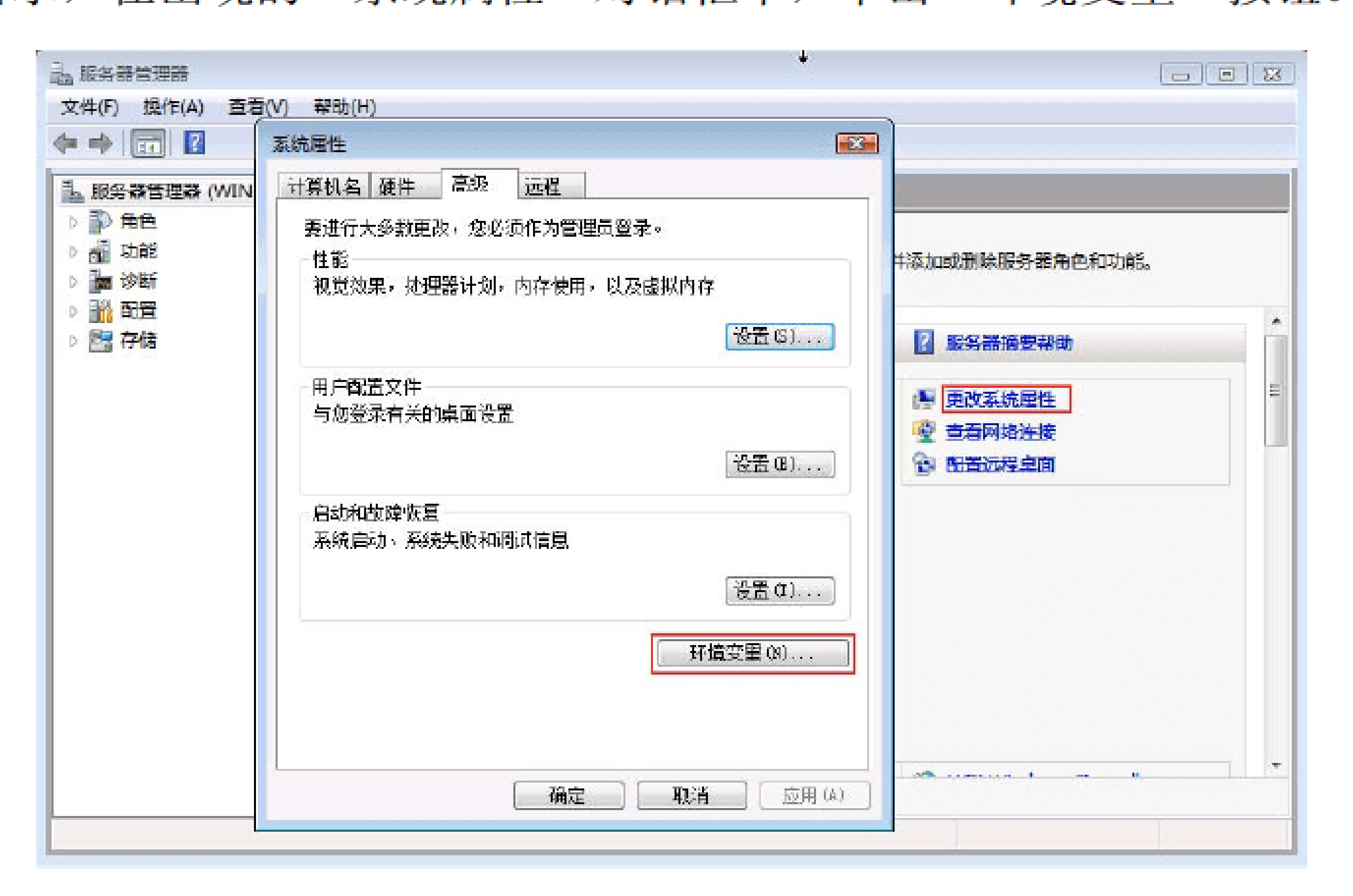


图 3-32　设置环境变量

③ 如图 3-33 所示，单击“编辑”按钮，将 TEMP 和 TMP 指向新的路径。指定的位置必须提前创建。

④ 选中系统变量 Path，单击“编辑”按钮。

⑤　如图 3-34 所示，在后面添加“;e:\app”。路径之间需要用“;”隔开。

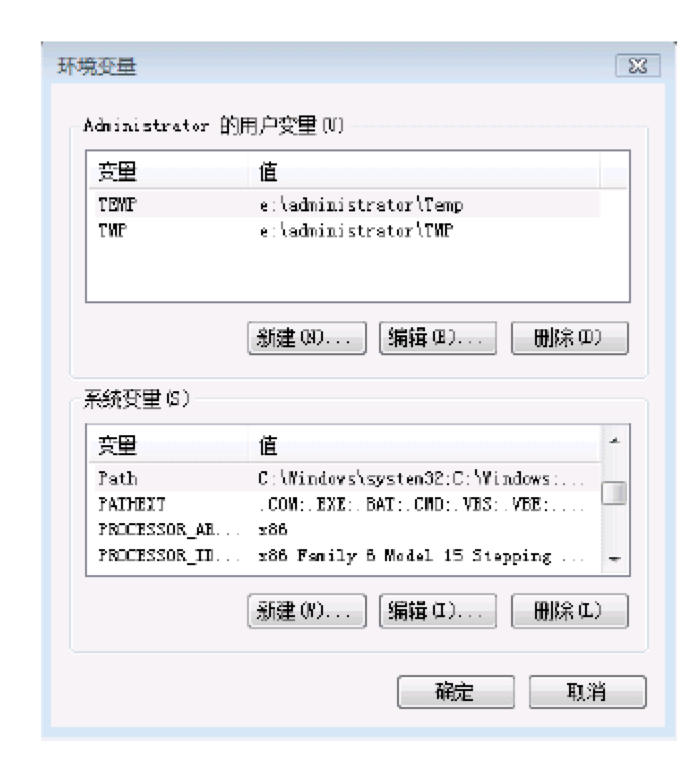




图 3-33　用户变量和系统变量

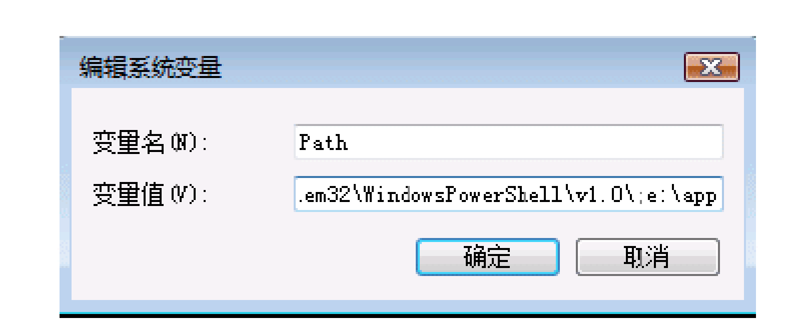


图 3-34　更改 Path 变量

3.5.4　任务 4：使用系统配置排除系统故障

系统配置是一种高级工具，可以帮助确定可能阻止 Windows 正常启动的问题。可以在禁用常用服务和启动程序的情况下 启动 Windows，然后再启用这些服务和程序；可以使用二分法快速找到导致问题的服务或程序，二分法即先禁用一半服务和程序，看看是否正常，如果正常，再禁用另一半的服务或程序，这样很快就能找到引起问题的服务或程序。如果禁用某个服务时没有出现问题，但是启用后出现问题，则可能是此服务导致出现这个问题。

系统配置用于查找并隔离问题，但并不表示它是启动管理程序。

若要永久删除或者关闭在启动时运行的程序或服务，选择“开始”→“运行”命令，在打开的“运行”对话框中输入 msconfig，可以打开系统配置工具。

下面说明系统配置中可用的选项卡和选项。

1. 常规

此选项卡中列出了启动配置模式的选项，如图 3-35 所示。

- 正常启动。以通常方式启动 Windows。使用其他两种模式解决问题后，使用此模式启动 Windows。
- 诊断启动。在只使用基本的服务和驱动程序的情况下启动 Windows。此模式可以帮助排除基本 Windows 文件造成此问题的可能性。
- 有选择的启动。在使用基本服务和驱动程序以及选择的其他服务和启动程序的情况下启动 Windows。

2. 启动

如图 3-36 所示，显示操作系统的配置选项和高级调试设置，包括以下内容。

- 最小：在仅运行关键系统服务的安全模式下启动 Windows 图形用户界面 (Windows Explorer)。网络已禁用。
- 其他外壳：在仅运行关键系统服务的安全模式下启动 Windows 命令提示。网络和图形用户界面已禁用。

- Active Directory 修复：在仅运行关键系统服务和 Active Directory 的安全模式下启动 Windows 图形用户界面。
- 网络：在仅运行关键系统服务的安全模式下启动 Windows 图形用户界面。网络已禁用。
- 无 GUI 启动：启动时不显示 Windows 初始屏幕。
- 启动日志：将启动进程中的所有信息都存储在%SystemRoot%Ntbtlog.txt 文件中。
- 基本视频：在最小 VGA 模式下启动 Windows 图形用户界面。这样会加载标准的 VGA 驱动程序，而不显示特定于计算机上视频硬件的驱动程序。
- OS 启动信息：显示启动过程中加载的驱动程序名称。
- 使所有启动设置成为永久设置：不跟踪在系统配置中所作的更改。之后可以使用系统配置更改选项，但是一定要手动更改。当选中该选项时，无法通过选择“常规”选项卡中的“正常启动”回滚更改。

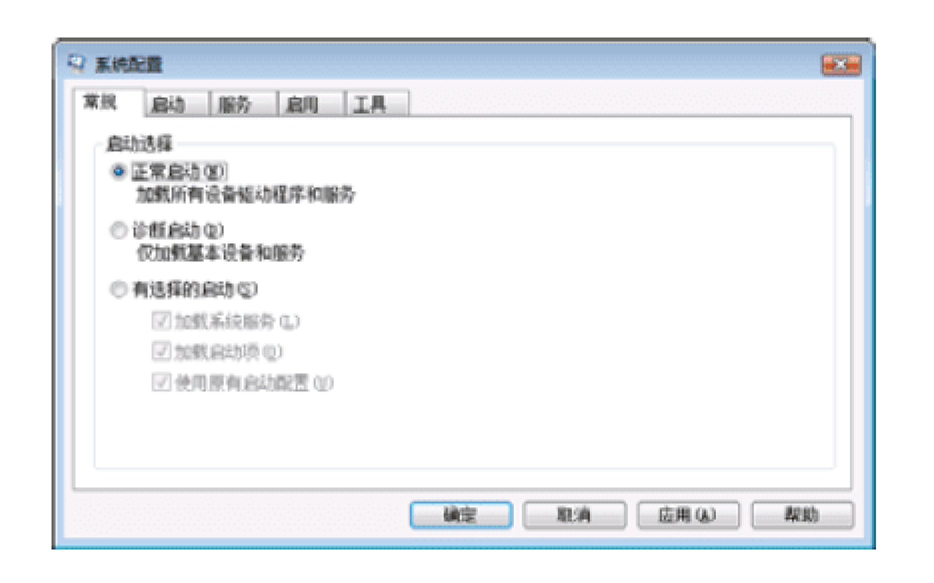


图 3-35　系统配置工具

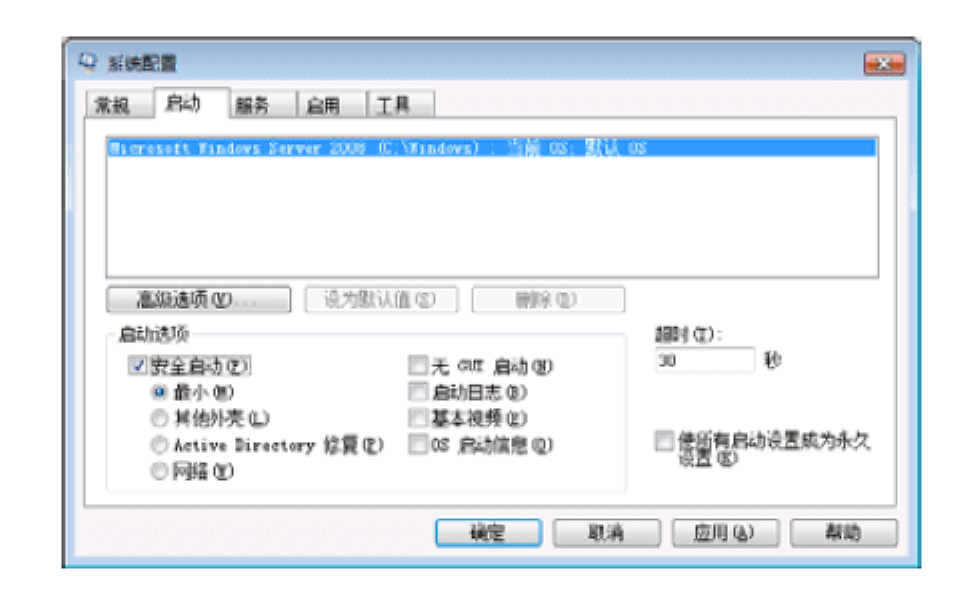


图 3-36　启动设置

3. 服务

如图 3-37 所示，列出计算机启动时启动的所有服务及其当前状态(“正在运行”还是“已停止”)。使用“服务”选项卡启用或禁用启动时的个别服务，以便查找可能引起启动问题的服务。

选中“隐藏所有 Microsoft 服务”复选框，在服务列表中仅显示第三方应用程序。取消选中某服务的复选框以便下次启动时禁用该服务。如果已选中“常规”选项卡中的“有选择的启动”单选按钮，必须选中“常规”选项卡中的“正常启动”单选按钮，或选中该服务的复选框以在启动时再次启动此服务。



警告：禁用启动时正常运行的服务可能会造成某些程序出现故障或导致系统不稳定。除非知道计算机操作不需要该列表中的服务，否则不要禁用这些服务。单击“全部禁用”将不会禁用某些操作系统启动时所需的安全的 Microsoft 服务。

4. 启用

如图 3-38 所示，列出计算机启动时运行的应用程序及其发行者的名称、可执行文件的路径、注册表项的位置或运行此应用程序的快捷方式。

取消选中某启动项的复选框以便下次启动时禁用该启动项。如果已选中“常规”选项卡中的“有选择的启动”，必须选择“常规”选项卡中的“正常启动”单选按钮，或选择该启动项的复选框以在启动时再次启动该启动项。

如果怀疑某个应用程序已经不太安全，应检查“命令”列查看该可执行文件的路径。

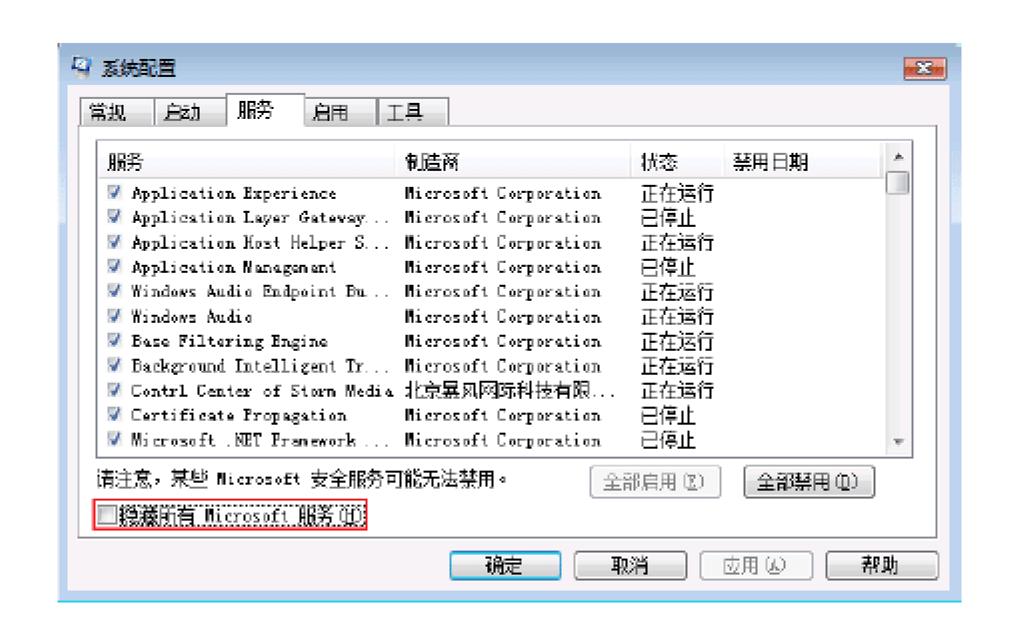


图 3-37　服务设置

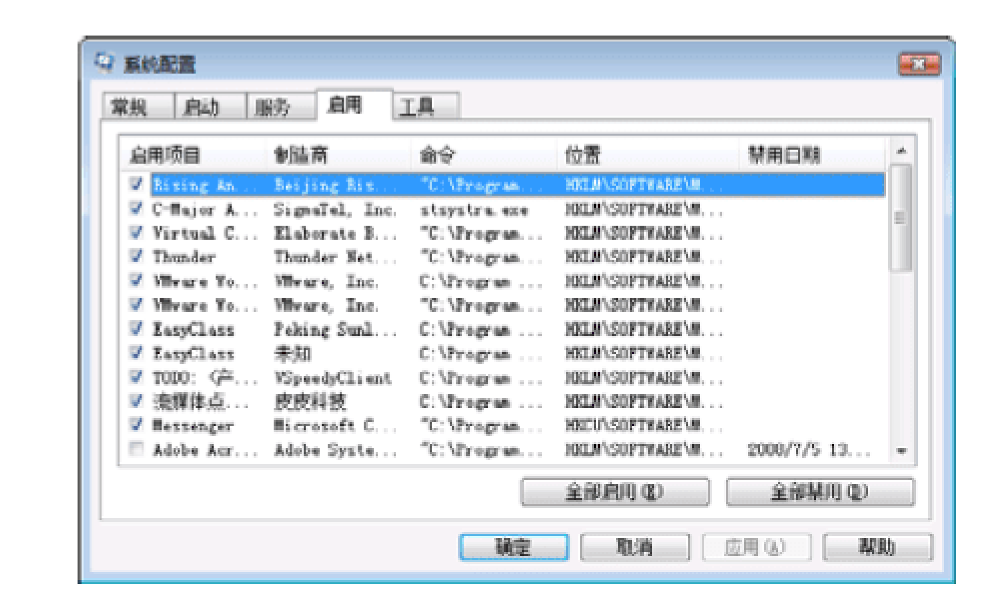


图 3-38　自动启动设置



注意：禁用启动时正常运行的应用程序可能会导致相关的应用程序启动速度变慢或者没有如期运行。

3.5.5　任务 5：配置文件夹选项

配置文件夹选项，显示隐藏的文件夹和系统文件夹，显示文件扩展名。

① 选择“开始”→“程序”→“设置”→“控制面板”命令，如图 3-39 所示，双击“文件夹选项”图标打开“文件夹选项”对话框，切换到“查看”选项卡。

② 如图 3-40 所示，取消选中“使用共享向导(推荐)”复选框。这样共享文件夹时就不会出现向导了。

③ 取消选中“隐藏受保护的系统文件(推荐)”复选框。如果想查看系统文件的话，可以显示出来。

④ 取消选中“隐藏已知文件类型的扩展名”复选框。这样就可以看到文件的扩展名了。

注意：文件夹选项只对当前用户生效。



图 3-39　文件夹选项

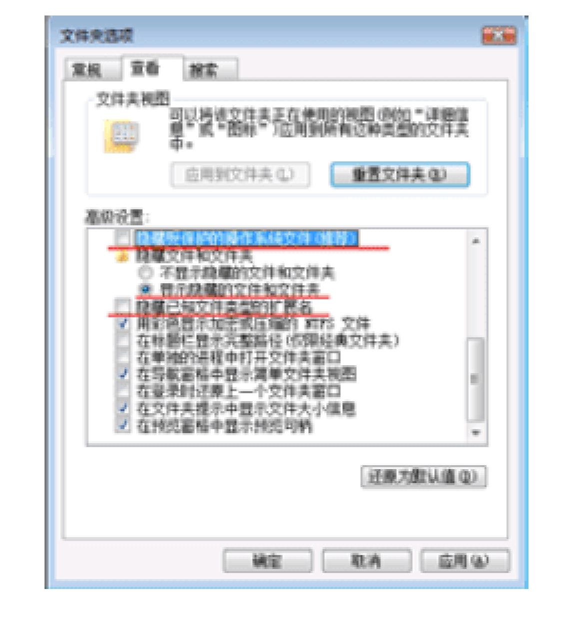


图 3-40　设置文件夹显示

3.6　实战 3：配置 IE 选项

任务描述

能够配置 IE 浏览器的主页，添加/删除搜索提供程序，配置 IE 浏览器的安全和仿冒网站过滤，能够改

变浏览器的增强的安全配置，能够学会配置 IE 浏览器使用代理服务器。

实战环境

- Windows Server 2008 企业版操作系统。
- 能够连接到 Internet。

实战目标

- 设置 IE 浏览器的主页。
- 增加搜索提供程序。
- 配置增强的安全配置和启用仿冒网站过滤器。
- 配置 IE 使用代理服务器。
- 不让 IE 关键时候“罢工”。

3.6.1 任务 1：定义 IE 浏览器主页和搜索提供程序

① 右击桌面上的图标，在弹出的快捷菜单中选择“属性”命令，打开“Internet 属性”对话框。IE 7.0 支持多个主页，可以输入欲打开 IE 默认访问的网站，如图 3-41 所示，每一行输入一个网址。

② 在“搜索”选项组中，单击“设置”按钮，打开“更改搜索默认值”对话框，如图 3-42 所示，可以指定默认的 IE 搜索提供程序。

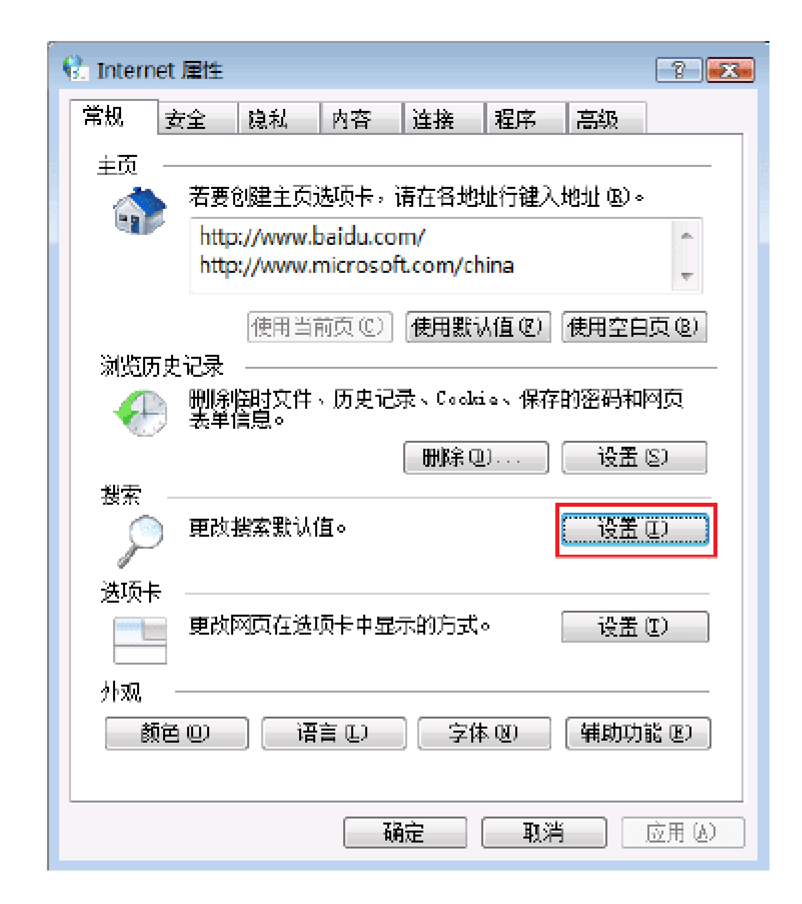


图 3-41 设置 IE 首页

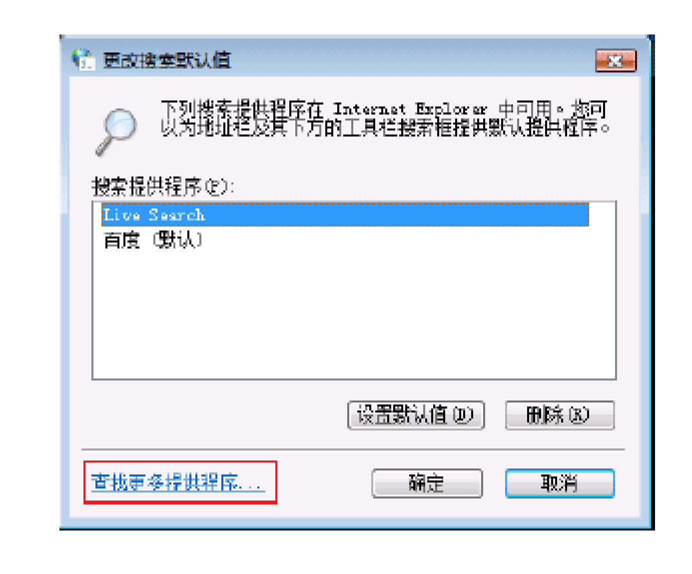


图 3-42 设置搜索提供程序

③ 在“更改搜索默认值“对话框中，如图 3-42 所示，单击“查找更多提供程序”按钮。

④ 在打开的网页中，如图 3-43 所示，单击 Google 选项，则可以“创建你自己的”搜索提供程序。注意观察现在的搜索默认提供程序是“百度”。

⑤ 如图 3-44 所示，在打开的对话框中，选中“将它设置为默认搜索提供程序”复选框，单击“添加提供程序”按钮。

⑥ 关闭 IE 浏览器，双击桌面上的图标，打开 IE 浏览器，如图 3-45 所示。注意：现在默认打开两个主页，默认搜索提供程序是 Google。

⑦ 如图 3-46 所示，输入“奥运会”，单击图标就能在 Google 上搜到与“奥运会”相关的信息。



图 3-43　添加搜索引擎

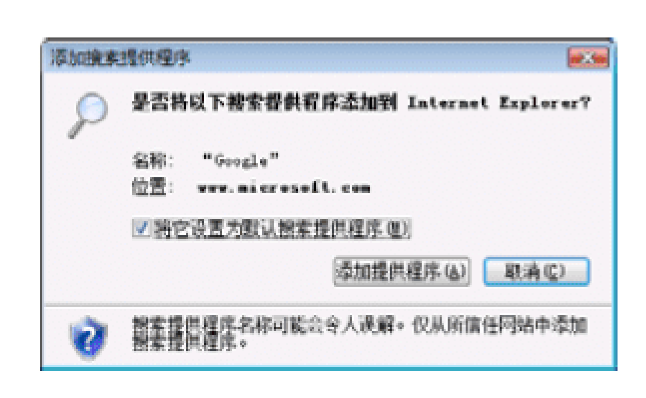


图 3-44　添加搜索提供程序



图 3-45　更改搜索提供程序



图 3-46　使用 Google 搜索引擎

3.6.2　任务 2：设置 IE 安全并打开自动仿冒网站筛选器

联机仿冒(Phishing 发音为 fishing)是通过欺诈电子邮件或网站来诱使计算机用户透露个人信息或财务信息的伎俩。常见联机仿冒骗局从看似来自受信任源的官方通知的电子邮件开始，如银行、信用卡公司或可信的在线商店。在电子邮件中，收件人被定向到要求提供个人信息(例如账号或密码)的欺骗性网站。该信息通常用于身份偷窃。

① 在 IE 浏览器属性对话框中，切换到“安全”选项卡。单击 Internet、“本地 Intranet”、“可信站点”和“受限站点”，可以看到有不同的安全级别，分别如图 3-47～图 3-50 所示。并且这些区域的安全级别不能调整，因为默认启用了增强的安全配置，在后面步骤将会为管理员去掉增强的安全配置。

② 选中“打开自动仿冒网站筛选器”单选按钮，如图 3-51 所示，在出现的最前端提示对话框中单击“关闭”按钮。

③ 这样 IE 浏览器将在高安全下浏览该网站，如图 3-52 所示，此时很多功能受限，比如 Flash 动画不能播放，脚本不能运行，不能下载东西。

④ 如图 3-53 所示，单击 IE 浏览器“工具”按钮，在弹出的下拉菜单中选择“Internet 选项”命令，打开“Internet 选项”对话框。

⑤ 在“Internet 选项”对话框中，如图 3-54 所示，选中“可信站点”选项，单击“站点”按钮。

⑥ 如图 3-55 所示，将 www.inhe.net 网站加入到“可信站点”。

⑦ 再次刷新 www.inhe.net 网站，发现网页中的图片能动了，但是 gif 的图片不能显示。

⑧ 如图 3-56 所示，单击 IE 浏览器“工具”按钮，在弹出的下拉菜单中选择“仿昌网站筛选”→“打开自动网站检查”命令。



图 3-47 Internet 区域安全级别



图 3-48 本地 Intranet 区域安全级别

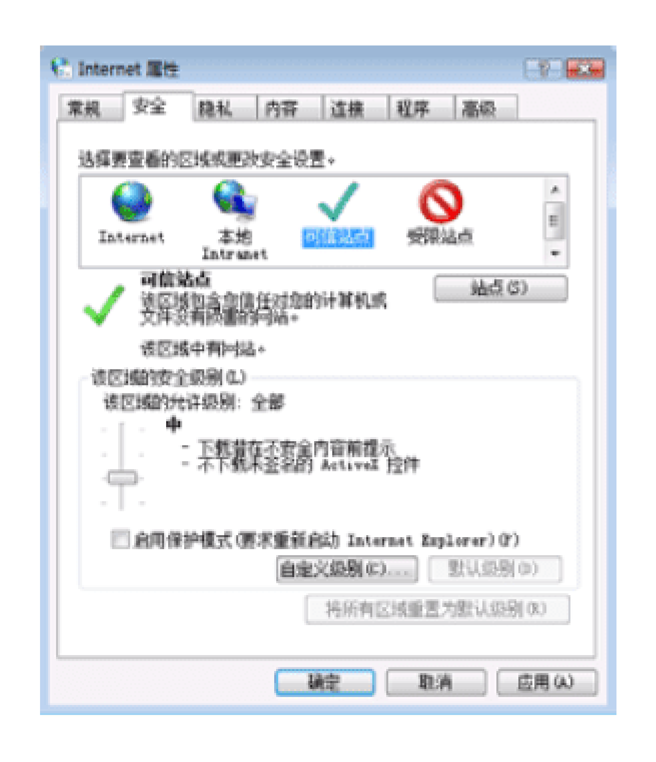


图 3-49 可信站点的安全级别

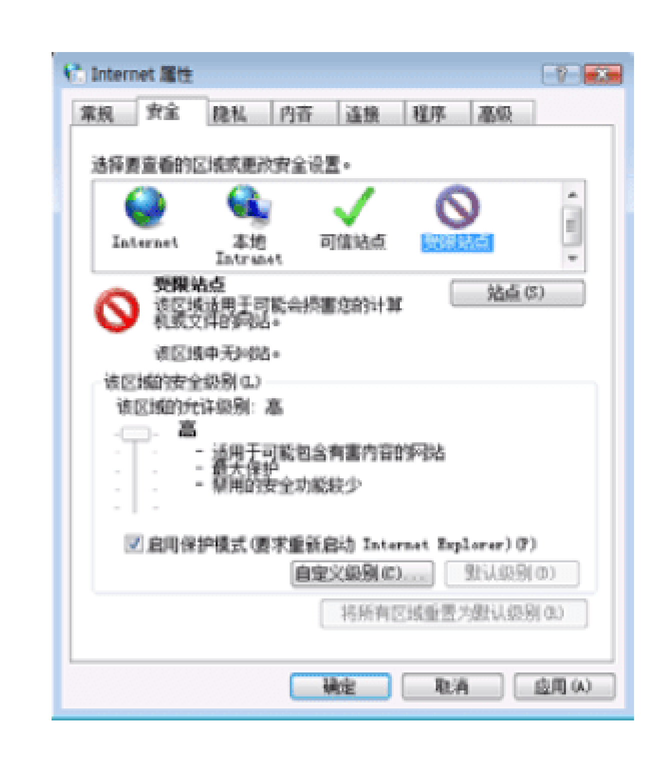


图 3-50 受限站点的安全级别

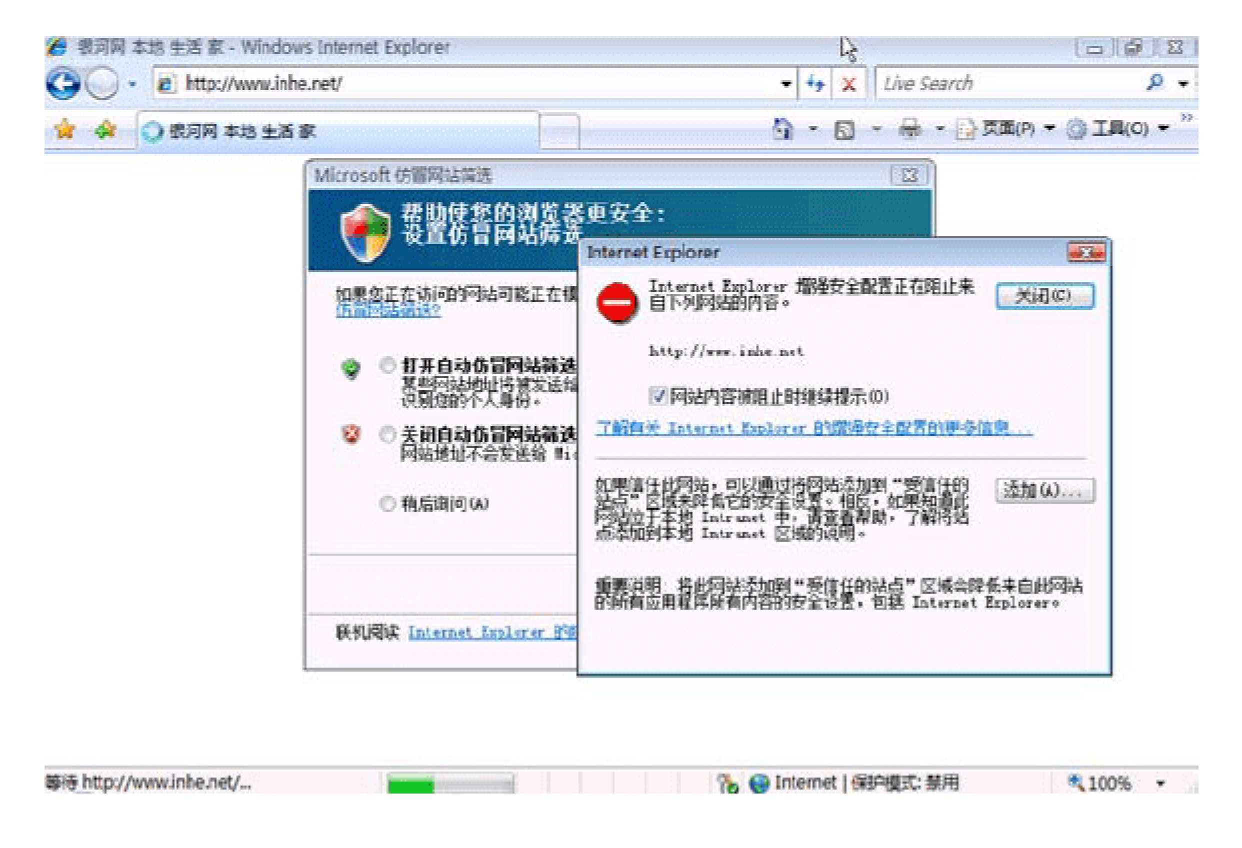


图 3-51 Internet 默认安全级别



图 3-52 默认的安全级别 Flash 不能播放

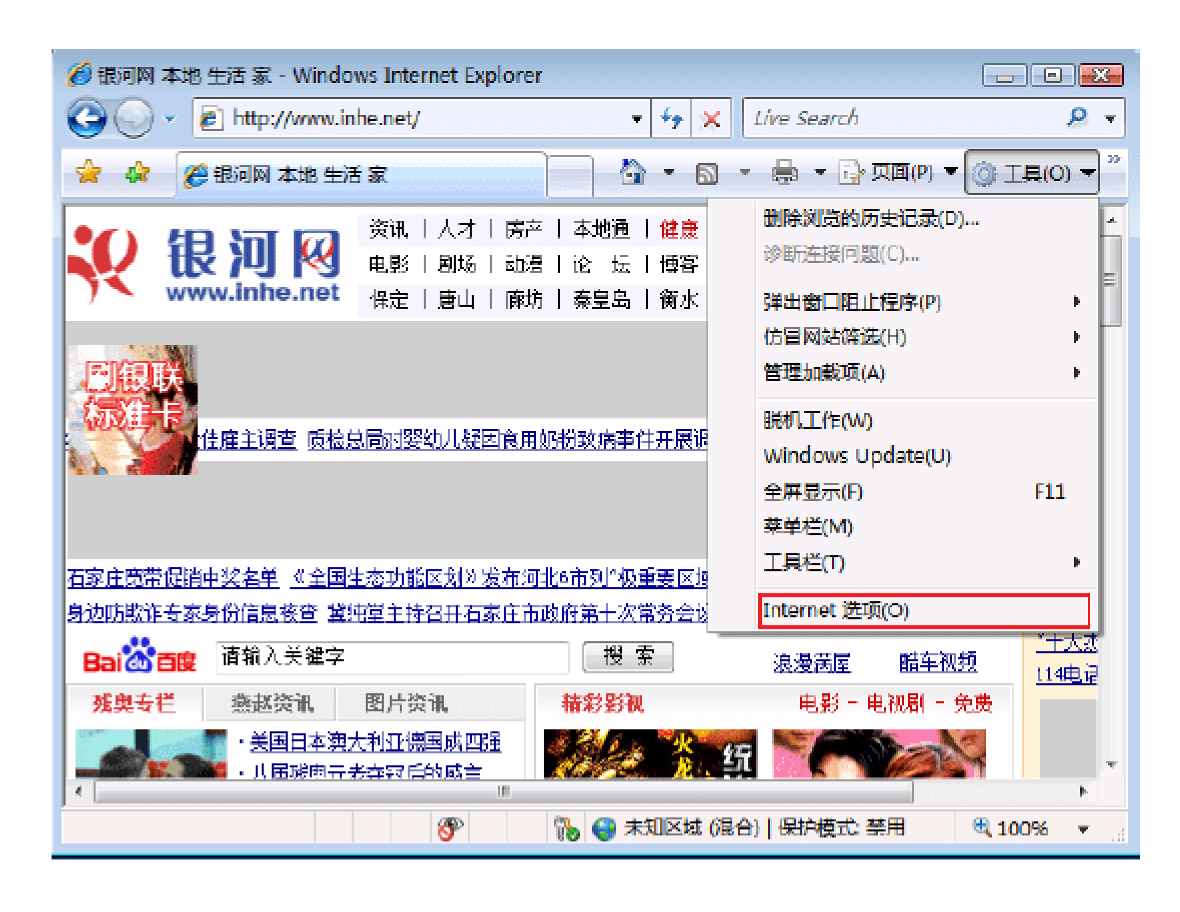


图 3-53　选择“Internet 选项”命令



图 3-54　管理可信站点

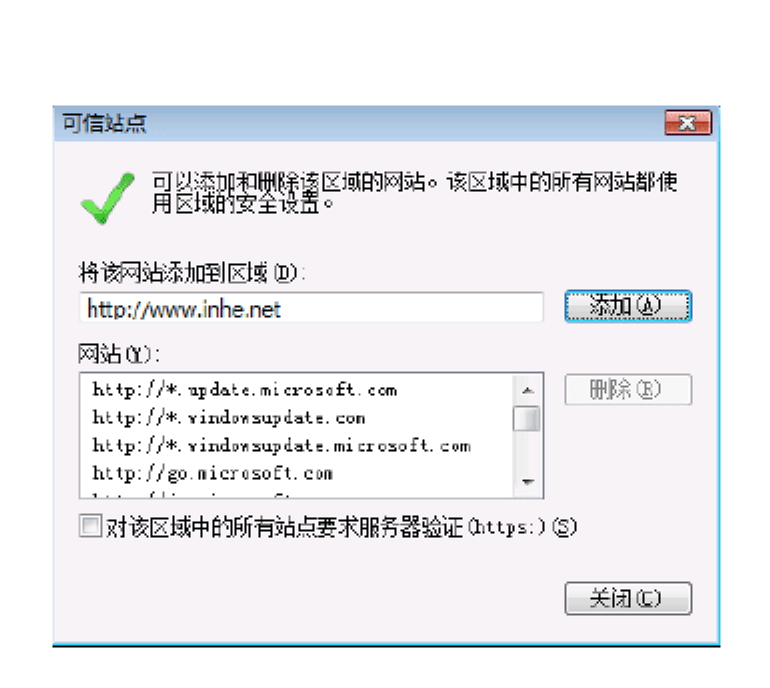


图 3-55　将银河网址添加到受信站点

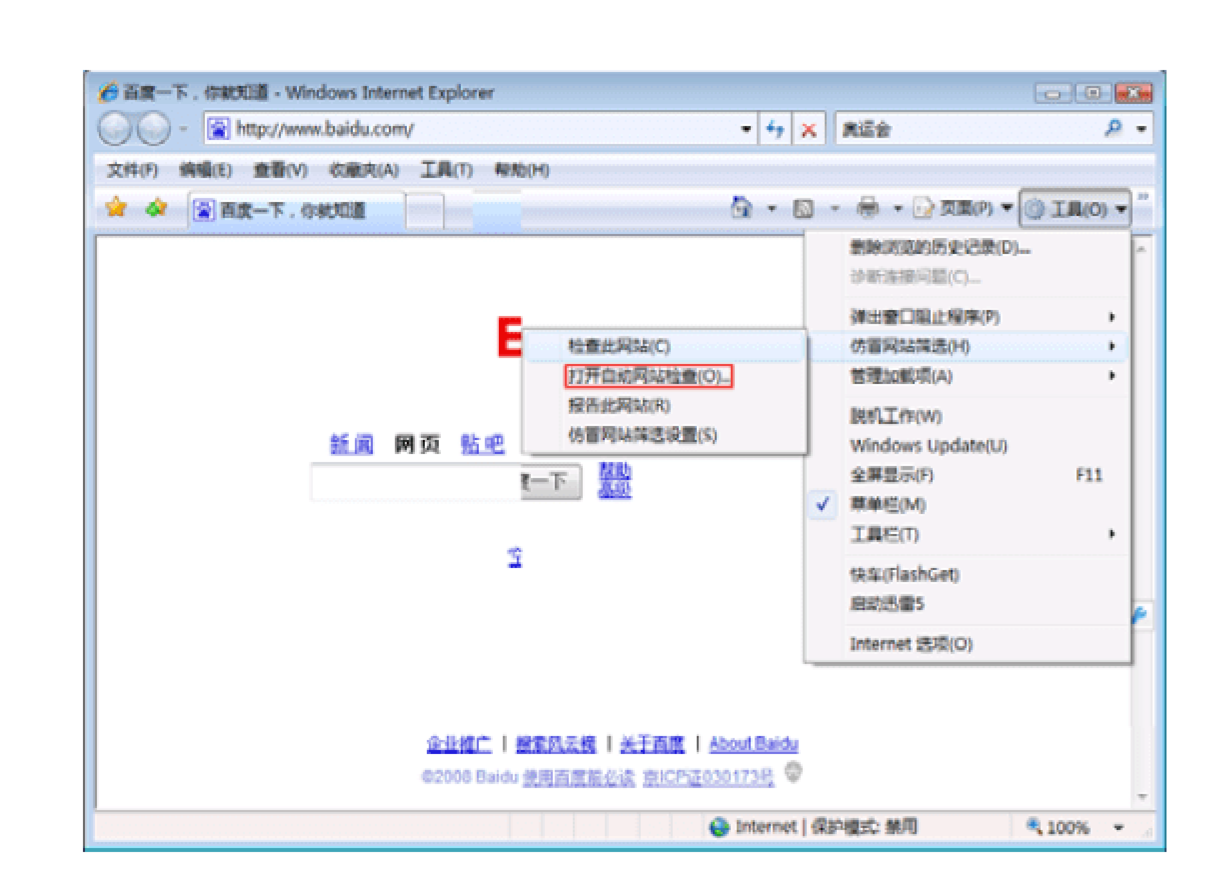


图 3-56　选择“打开自动网站检查”命令

3.6.3　任务 3：禁用 Internet Explorer 增强的安全配置

Internet Explorer 增强的安全配置 (IE ESC) 采用一种方式配置你的服务器和 Microsoft Internet Explorer，从而降低服务器受 Web 内容和应用程序脚本潜在攻击的暴露程度。通过提高 Internet Explorer 安全区域上的默认安全级别并且更改默认设置来实现此功能。

① 关闭 Internet Explorer 的所有实例。

② 打开“服务器管理器”窗口。如图 3-57 所示，在“安全信息”下，单击“配置 IE ESC”按钮。

③ 若要禁用 IE ESC，如图 3-58 所示，在“管理员”选项区，选中“禁用”单选按钮，在“用户”选项区，选中“启用(推荐)”单选按钮。然后单击“确定”按钮。

④ 再次访问 www.inhe.net，发现一切正常。

⑤ 再次打开“Internet 选项”对话框，查看 Internet 的安全级别，如图 3-59 所示，现在可以调整各区域的安全级别了。现在可像 Windows Vista 一样访问 Internet 网站了。

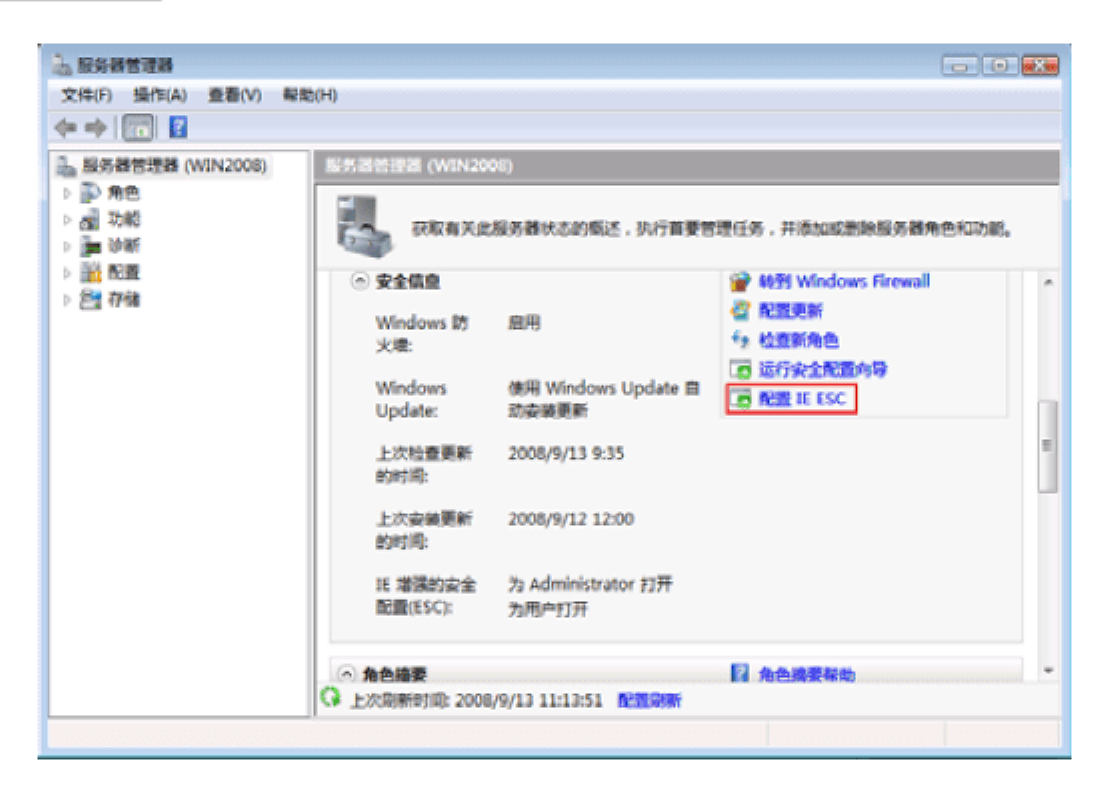


图 3-57　配置 IE ESC

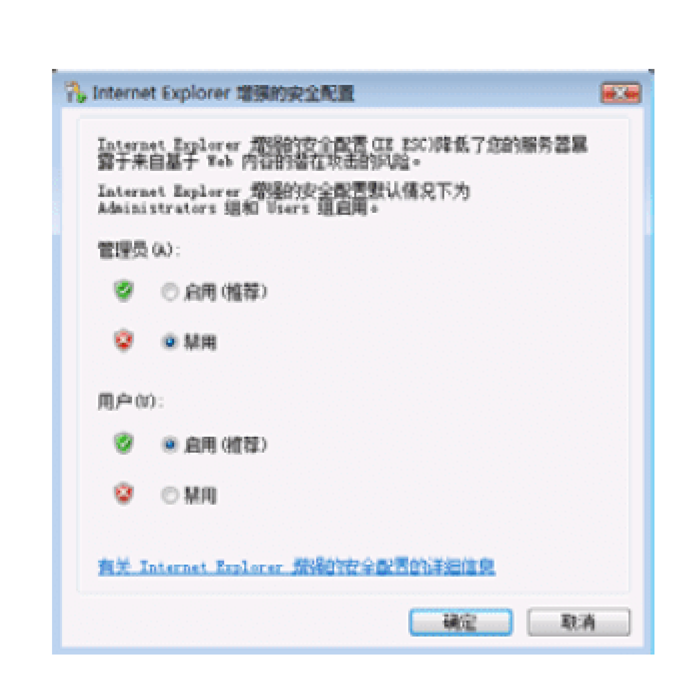


图 3-58　禁用增强的安全配置

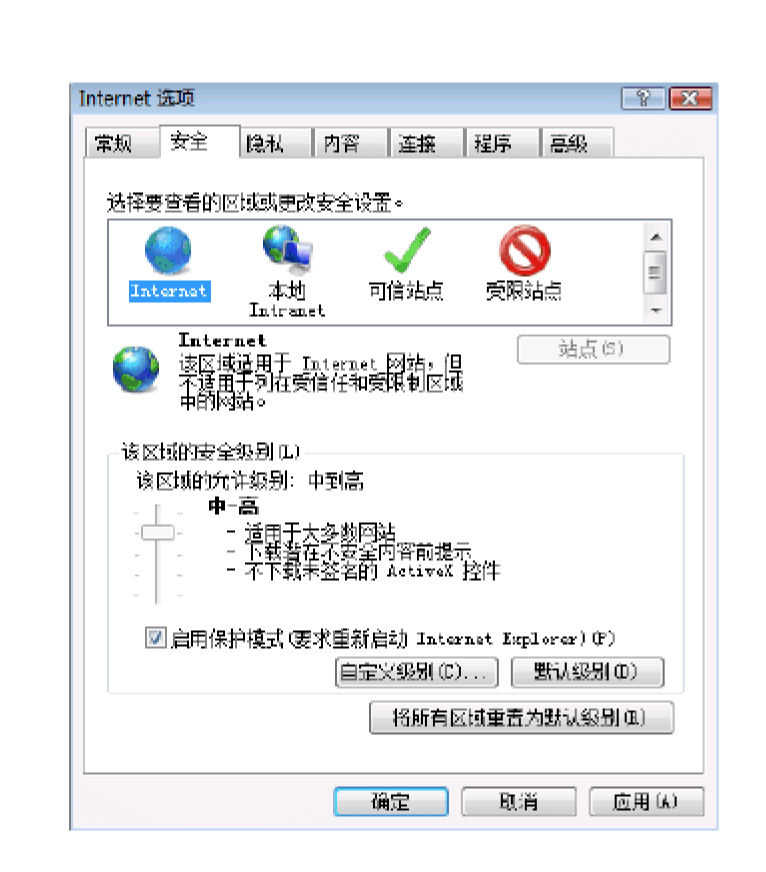
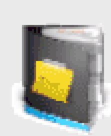


图 3-59　调整各个区域安全级别

3.6.4　任务 4：配置 IE 使用代理

代理服务器是在 Web 浏览器(如 Internet Explorer)和 Internet 之间起媒介作用的计算机。代理服务器通过存储经常使用的网页副本来提高 Web 性能。当浏览器请求存储在代理服务器收集(其缓存)中的网页时，网页由代理服务器提供，这比进入 Web 的速度要快。通过过滤掉某些 Web 内容和恶意软件，代理服务器还可以提高安全性。著名的代理软件有微软的 ISA 2006 和 CCproxy。



提示：代理服务器多数由组织和公司中的网络使用。通常，从家中连接到 Internet 的用户不使用代理服务器。

① 在如图 3-60 所示的“Internet 选项”对话框的“连接”选项卡中，单击“局域网设置”按钮。

② 如图 3-61 所示，在“局域网(LAN)设置”对话框的“地址”文本框中，输入代理服务器的地址。

③ 在“端口”文本框中，输入端口号。

④ 如果网络对不同的服务(如 HTTP、HTTPS 或 FTP)需要单独的代理地址，可单击“高级”按钮，然后输入要使用的单独代理服务器地址，如图 3-62 所示。

⑤ 访问企业内部网站不需要使用代理，在“例外情况”选项区域中，输入那些直接访问的网址。



图 3-60　设置连接设置

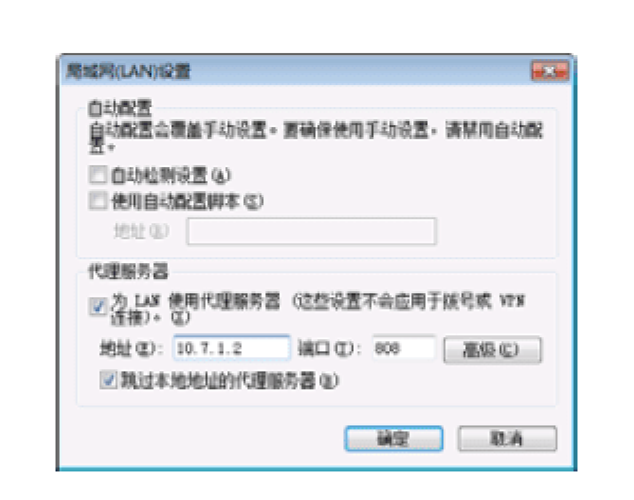


图 3-61　指定代理服务器和端口

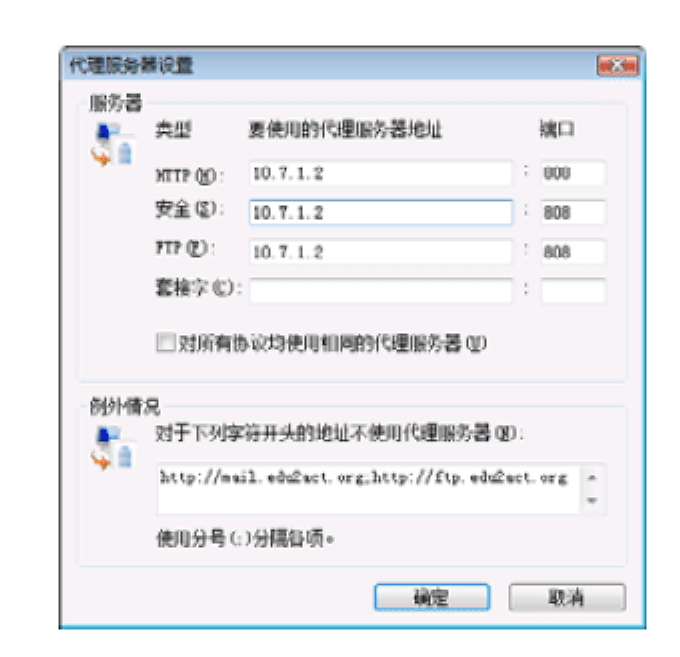


图 3-62　代理服务器设置

⑥　完成更改后，单击“确定”按钮，直到返回 Internet Explorer。

3.6.5　任务 5：不让 IE 关键时候“罢工”

不少网络管理员反映，在 Windows Server 2008 系统环境下，使用 Internet Explorer 浏览器上网访问内容时，常常在页面内容打开到一半的时候，IE 浏览器窗口出现突然关闭的现象，很显然这种现象如果频繁出现的话，自然会降低上网冲浪的效率。为了有效地提高在 Windows Server 2008 系统环境下的上网访问效率，可以按照如下步骤来避免 IE 浏览器窗口发生自动关闭现象。

①　首先以超级用户权限进入 Windows Server 2008 系统，然后右击该系统桌面中的 Internet Explorer 程序图标，在弹出的快捷菜单中选择“Internet 属性”命令，打开“Internet 属性”对话框。

②　如图 3-63 所示，单击“安全”标签，打开“安全”选项卡，选中 Internet 选项，并取消选中“启用保护模式(要求重新启动 Internet Explorer)”复选框。之后，按照相同的操作方法，选中“本地 Intranet”选项，取消选中“启用保护模式(要求重新启动 Internet Explorer)”复选框。

③　若经过上面的设置，Internet Explorer 浏览器仍然会在关键时刻“罢工”，则不妨单击“Internet 属性”对话框中的“高级”标签，切换到“高级”选项卡，如图 3-64 所示。单击“重置”按钮，这样 Internet Explorer 浏览器的工作状态就会恢复到原始状态，此时 IE 浏览器在关键时候就不会再“罢工”了。



图 3-63　取消保护模式

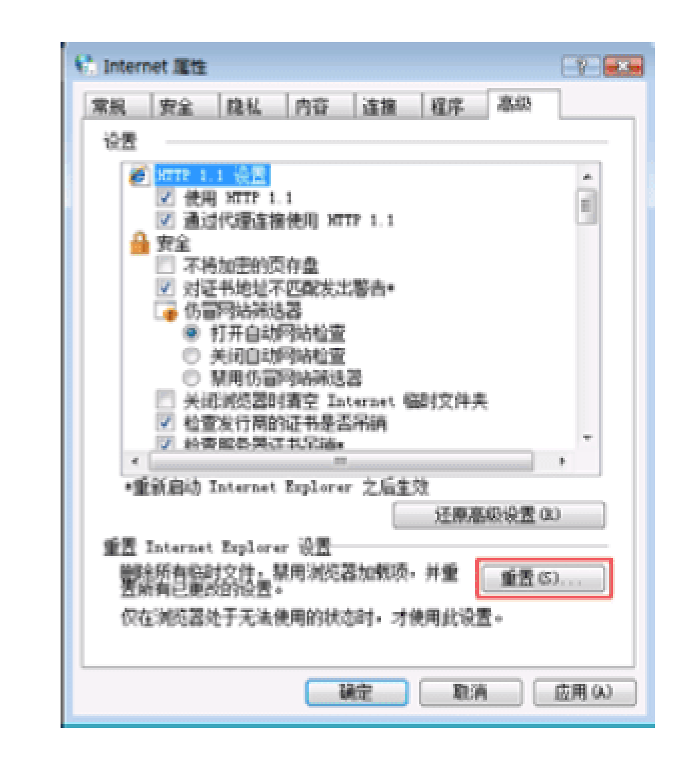


图 3-64　重置 IE 浏览器

3.7 实战 4：配置反间谍软件 Windows Defender

间谍软件是可以自行安装的软件，或者未提供足够通知、同意或控制就在计算机上运行的软件。间谍软件在感染计算机后可能不显示任何症状，但许多类型的恶意软件或不需要的程序都可以影响计算机的运行方式。例如，间谍软件可以监视在线行为，或者收集有关用户的信息(包括个人标识或其他敏感信息)，更改计算机设置或降低计算机的运行速度。

在使用计算机的同时运行反间谍软件非常重要。间谍软件和其他可能不需要的软件会在用户连接到 Internet 时尝试自行安装到计算机上。如果使用 CD、DVD 或其他可移动介质安装程序，它也会感染计算机。不需要的或恶意软件并非仅在安装后才能运行，它还会被编程为随时运行。

3.7.1 如何知道计算机上有间谍软件或不需要的软件

在以下情况下，计算机上可能有某种形式的间谍软件。

- 通知无意添加到 Web 浏览器的新工具栏、链接或收藏夹。
- 默认的主页、鼠标指针或搜索程序更改。
- 输入特定网站(如搜索引擎)的地址，但未予通知即转到另一网站。
- 看到弹出广告，即使未在 Internet 上。
- 计算机突然开始启动或运行缓慢。

即使未发现任何症状，计算机上也可能有间谍软件。这种软件可以在未经认可或同意的情况下，收集关于用户和计算机的信息。只要使用计算机即运行 Windows Defender 可有助于发现和删除此类软件。

3.7.2 如何防止间谍软件感染计算机

下面几种方法可防止间谍软件感染计算机。

- 运行最新的防间谍软件。此 Windows 版本所附的 Windows Defender 有助于防止在计算机上自行安装或运行恶意软件、间谍软件和其他可能不需要的软件或广告软件。可以自动发现和删除可能已安装的恶意软件。
- 使计算机保持在最新状态。Microsoft 通常发布安全更新来帮助防止在未经确认的情况下安装间谍软件。大多数新的防病毒程序都有间谍软件保护，也应将其保持在最新状态。推荐启用 Windows 自动更新，并定期更新间谍软件和防病毒程序。
- 安装软件前检查许可协议。访问网站时，不自动同意下载站点提供的任何内容。如果下载免费软件，如文件共享程序或屏幕保护程序，应详细阅读许可协议。查找必须接受公司广告和弹出页面的条款，或者软件将某些信息发回软件发行者的条款。

Windows Defender 提供了 3 种途径来帮助阻止间谍软件和其他可能不需要的软件感染计算机。

- 实时保护。当间谍软件或其他可能不需要的软件试图在计算机上自行安装或运行时，Windows Defender 会发出警报。如果程序试图更改重要的 Windows 设置，它也会发出警报。
- SpyNet 社区。联机 Microsoft SpyNet 社区可帮助查看其他人是如何响应未按风险分类的软件的。查看社区中其他成员是否允许使用此软件，能够帮助选择是否允许此软件在计算机上运行。

同样，如果加入社区，用户的选择也将添加到社区分级以帮助其他人作出选择。

- 扫描选项。使用 Windows Defender 可以扫描可能已安装到计算机上的间谍软件和其他可能不需要的软件；定期计划扫描，还可以自动删除扫描过程中检测到的任何恶意软件。

使用 Windows Defender 时，更新定义非常重要。定义是一些文件，它们就像一本不断更新的有关潜在软件威胁的百科全书。Windows Defender 使用这些定义来确定它所检测的软件是否为间谍软件或其他可能不需要的软件，然后发出警报提示潜在风险。为了帮助用户保持定义为最新，Windows Defender 与 Windows Update 一起运行，以便在发布新定义时自动进行安装。另外，还可将 Windows Defender 设置为在扫描之前联机检查更新的定义。

3.7.3　任务：配置 Windows Defender

下面的实战将配置 Windows Defender 反间谍软件，启用实时监控和自动更新。

① 如图 3-65 所示，打开“控制面板”窗口，单击 Windows Defender 选项。

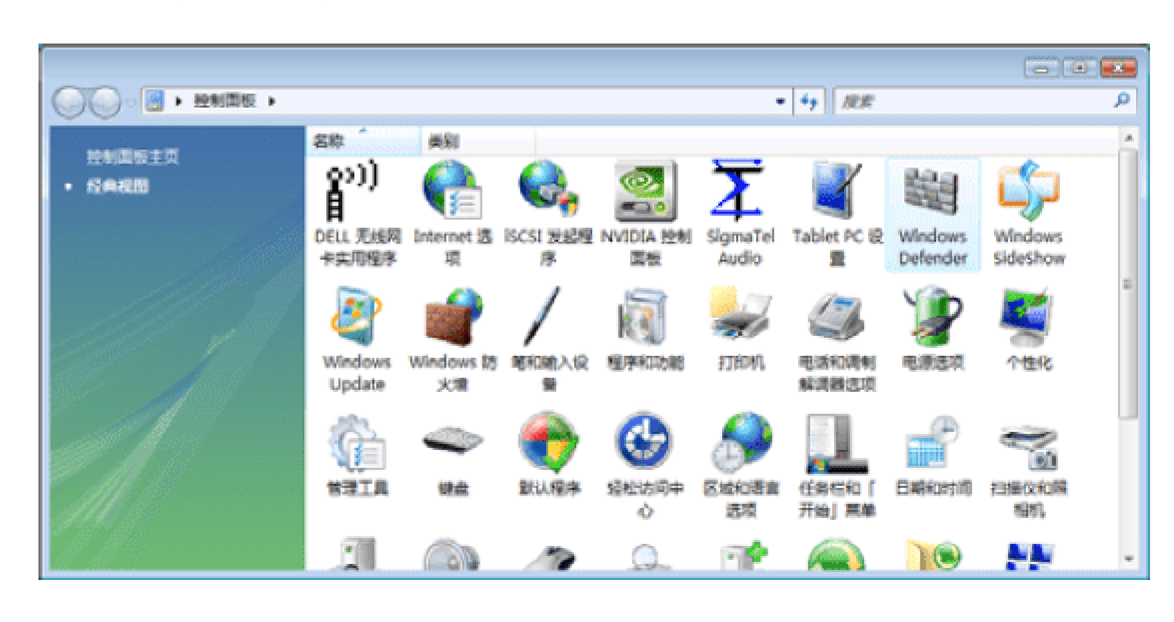


图 3-65　打开 Windows Defender

② 如图 3-66 所示，在 Windows Defender 窗口中，选择“工具”→“选项”命令。

③ 如图 3-67 所示，配置每天自动扫描，选中“扫描前检查更新的定义”和“扫描过程中将默认操作应用到检测到的项目”复选框。

④ 默认操作，“高警报项目”选择删除，“中等警报项目”选择删除，“低警报项目”选择默认操作。



图 3-66　设置 Windows Defender

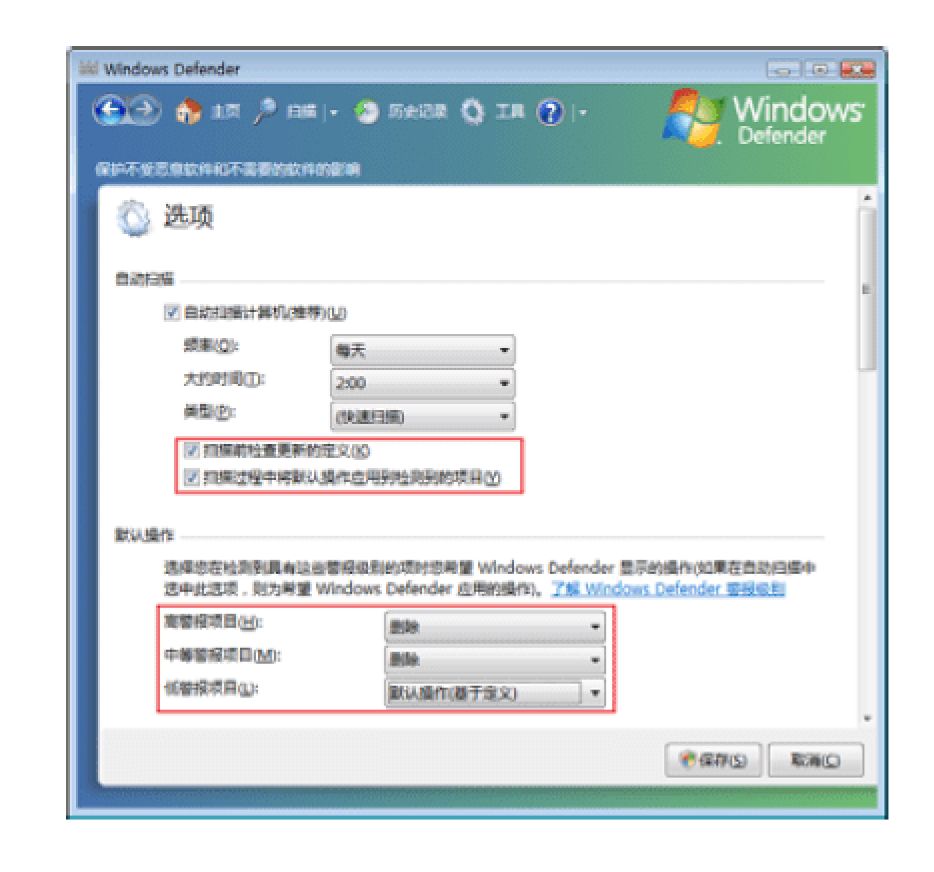


图 3-67　配置扫描频率以及采取的措施

⑤　如图 3-68 所示，配置“实时保护选项”和“高级选项”。

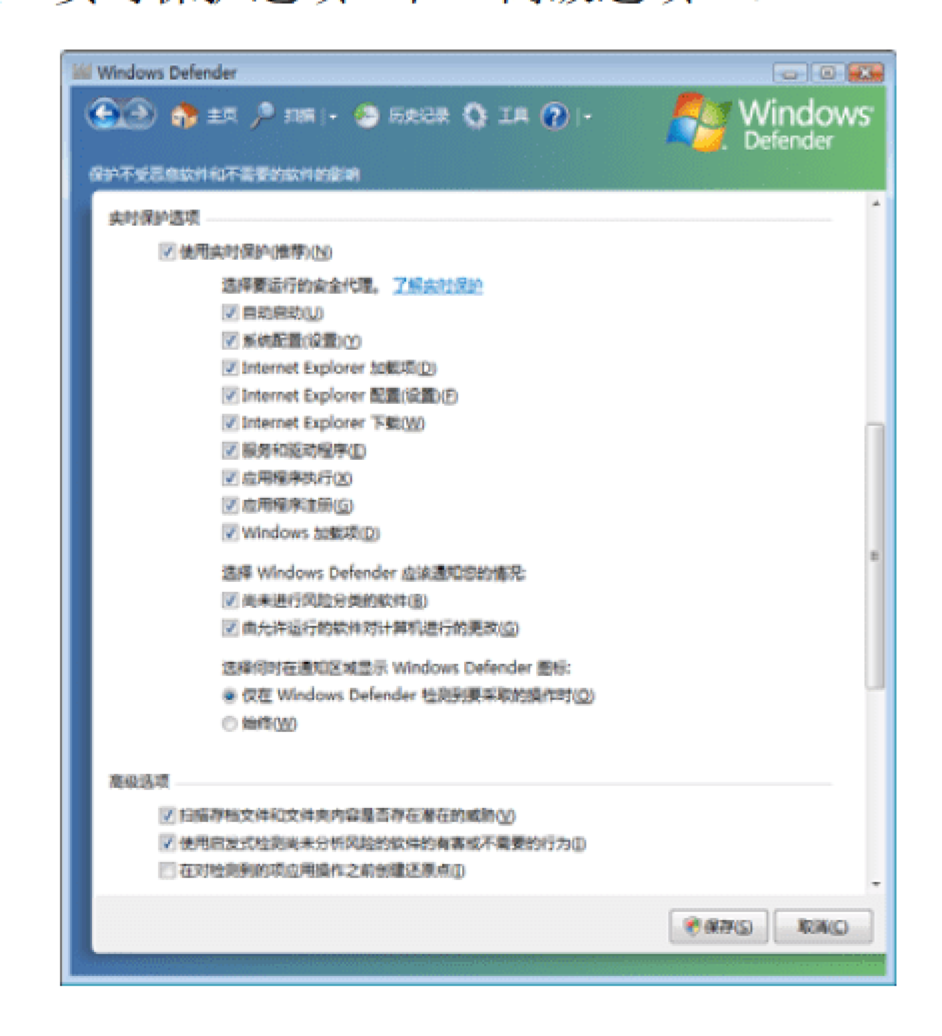


图 3-68　配置“实时保护选项”和“高级选项”

3.8　配置网络中心

3.8.1　选择网络位置

第一次连接到网络时，必须选择网络位置。这将为所连接网络的类型自动设置恰当的防火墙设置。如果用户在不同的位置(例如，家庭、本地咖啡店或办公室)连接到网络，则选择一个网络位置可帮助确保始终将计算机设置为适当的安全级别。

有 3 个网络位置：家庭、办公室和公共场所。

- 家庭或办公室：如果用户认识并信任网络上的人和设备，可为家庭或小型办公网络选择以上位置中的任一位置。默认情况下，网络发现处于启用状态，它允许你查看网络上的其他计算机和设备并允许其他网络用户查看你的计算机。有关详细信息，可参阅什么是网络发现。
- 公共场所：为公共场所(例如，咖啡店或机场)中的网络选择此位置。此位置旨在使你的计算机对周围的计算机不可见，并且帮助保护计算机免受来自 Internet 的任何恶意软件的攻击。对此位置禁用网络发现。

**注意：**如果网络上只有一台计算机并且你无须共享文件或打印机，则最安全的选择是“公共场所”。

1. Windows 防火墙如何影响网络位置

当在公共场所连接到网络时，“公共场所”位置会阻止某些程序和服务运行，这样可帮助保护计算机阻止未授权的访问。如果连接到“公共场所”并且 Windows 防火墙处于打开状态，则某些程序或服务可能会要求用户对其解除阻止(允许其通过防火墙进行通信)，以便这些程序或服务可以正常工作。

如果对某个程序解除了阻止，则对于与当前连接到的网络具有相同位置类型的所有网络，Windows 防

火墙都将解除其对该程序的阻止。例如，如果在咖啡店连接到网络并选择“公共场所”作为位置类型，然后解除了对一个即时消息程序的阻止，则“公共场所”位置中的所有网络对该程序的阻止都将被解除。

如果在连接到公共网络时解除了对多个程序的阻止，可考虑将网络位置更改为“家庭”或“办公室”。相对于影响连接到的每个公共网络，这一更改操作可能会更安全。但应注意，如果进行了此更改，计算机将对网络上的其他人可见。

2. 允许程序通过防火墙有何风险

当在防火墙中创建一个例外或者打开一个端口时，便已允许某个特殊的程序从计算机通过防火墙发送或接收消息。允许程序通过防火墙进行通信(有时称为解除阻止)就像是在防火墙中打开了一扇很小的门。

每次为程序创建一个例外或打开一个端口以便其通过防火墙进行通信时，计算机的安全性也随之降低。防火墙拥有的例外或打开的端口越多，黑客或恶意软件使用这些通道传播蠕虫、访问文件或使用计算机将恶意软件传播到其他计算机的机会也就越大。

通常，创建程序例外比打开端口更为安全。如果打开一个端口，无论程序是否正在使用它，该端口都将始终保持打开状态，直到将其关闭。如果创建一个例外，这个“门”仅会在需要进行特殊通信时才打开。

降低安全风险建议如下。

- 仅在真正需要时创建例外或打开端口，并且删除不再需要的例外或关闭不再需要的端口。
- 切勿为不知道的程序创建例外或打开端口。

3. 什么是网络发现

网络发现是一种网络设置，该设置会影响你的计算机是否可以查看(找到)网络上的其他计算机和设置，以及网络上的其他计算机是否可以查看你的计算机。

存在以下三种网络发现状态。

- 启用。此状态允许你的计算机查看其他网络计算机和设备，并允许其他网络计算机上的用户查看你的计算机。这使共享文件和打印机变得更加容易。
- 禁用。此状态阻止你的计算机查看其他网络计算机和设备，并阻止其他网络计算机上的用户查看你的计算机。
- 自定义。这是一种混合状态，在此状态下与网络发现有关的部分设置已启用，但不是所有设置都启用。例如，可以打开网络发现，但是用户或系统管理员可能禁用了会影响网络发现的防火墙例外。

4. 通过公用文件夹共享文件

通过公用文件夹，可方便地共享计算机上保存的文件。可以与使用同一台计算机的其他用户和同一网络中使用其他计算机的用户共享此文件夹中的文件。放入公用文件夹的任何文件或文件夹都将自动与具有访问公用文件夹权限的用户共享。

- 哪些人可以访问公用文件夹

  拥有计算机的用户账户和密码的人都可以访问公用文件夹，但可以决定是否允许网络中的任何人访问公用文件夹。无法选择哪些人可以通过网络访问公用文件夹。要么将访问权限授予网络中的所有人，要么不授予任何人。但是，可以通过那些具有访问公用文件夹权限的用户来选择是否只能打开文件，或还可以更改和创建文件，来设置权限级别。

还可以打开密码保护的共享。这使只具有计算机的用户账户和密码的用户才具有对公用文件夹的网络访问权限。

- 公用文件夹中有什么

  在你或使用你的计算机的其他人向其添加文件之前，公用文件夹中不包含任何文件。公用文件夹包含若干子文件夹，这有助于你管理共享的文件。这些文件夹的大多数都是通过内容类型进行管理的，包括以下内容。

  - 公用文档。
  - 公用下载。
  - 公用音乐。
  - 公用图片。
  - 公用视频。

- 应在公用文件夹中放置什么

  这取决于你，但一般来说，应将要共享的任何文件或文件夹放到公用文件夹中，将要共享的歌曲复制或移动到公用音乐文件夹中，将图片复制或移动到公用图片文件夹等。甚至可以将 Internet Explorer 收藏夹复制到公用收藏夹文件夹中，使其他人能访问你的 Web 链接。公用文件夹是放置共享文件的合适位置，实现与授予了公用文件夹访问权限的用户共享文件。

  不应将不希望让他人看到或只希望某些人访问的文件放到公用文件夹中。可以通过非公用文件夹来共享它们。

3.8.2 任务 1：网络位置对访问网络资源的影响

任务描述

更改网络位置来保护计算机网络安全，清楚更改网络位置对访问网络资源的影响，掌握更改网络位置的意义。

本实战将更改 WebServer 的网络位置，在 Windows Server 2008 上测试 WebServer 网络位置变化对访问 WebServer 的影响。

实战环境

- Windows Server 2008 企业版操作系统 Windows Server 2008，IP 地址 10.7.10.114。
- Windows Server 2008 企业版操作系统 WebServer，IP 地址 10.7.10.102。

实战目标

- 清楚网络位置对网络安全的影响。
- 更改 WebServer 上的网络位置。
- 在 Windows Server 2008 上测试 WebServer 网络位置变化对访问 WebServer 的影响。

实战步骤如下。

① 在 WebServer 上，如图 3-69 所示，单击任务栏上的图标，单击“网络和共享中心”选项。

② 如图 3-70 所示，网络位置为“公用网络”，“网络发现”关闭，“文件共享”关闭，“公用文件夹共享”关闭，“打印机共享”关闭，“密码保护的共享”启用。

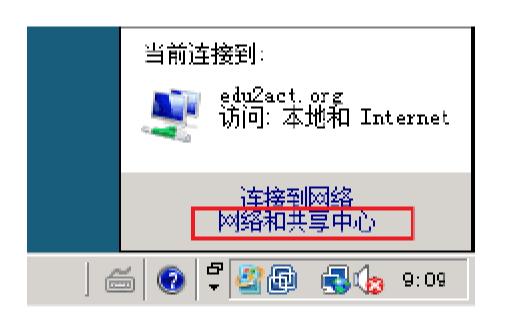


图 3-69　打开“网络和共享中心”



图 3-70　查看共享和发现

③　双击桌面上的“网络”图标，如图 3-71 所示，因关闭了“网络发现”，不能访问浏览到网络中的计算机。当然网络中的其他计算机也不能从网上发现这台计算机。

④　如图 3-72 所示，在 Windows Server 2008 上，ping 10.7.10.102 不通，在“运行”对话框中输入\\10.7.10.102，单击“确定”按钮，出现“网络错误”对话框，这表明不能访问 WebServer 的共享资源。

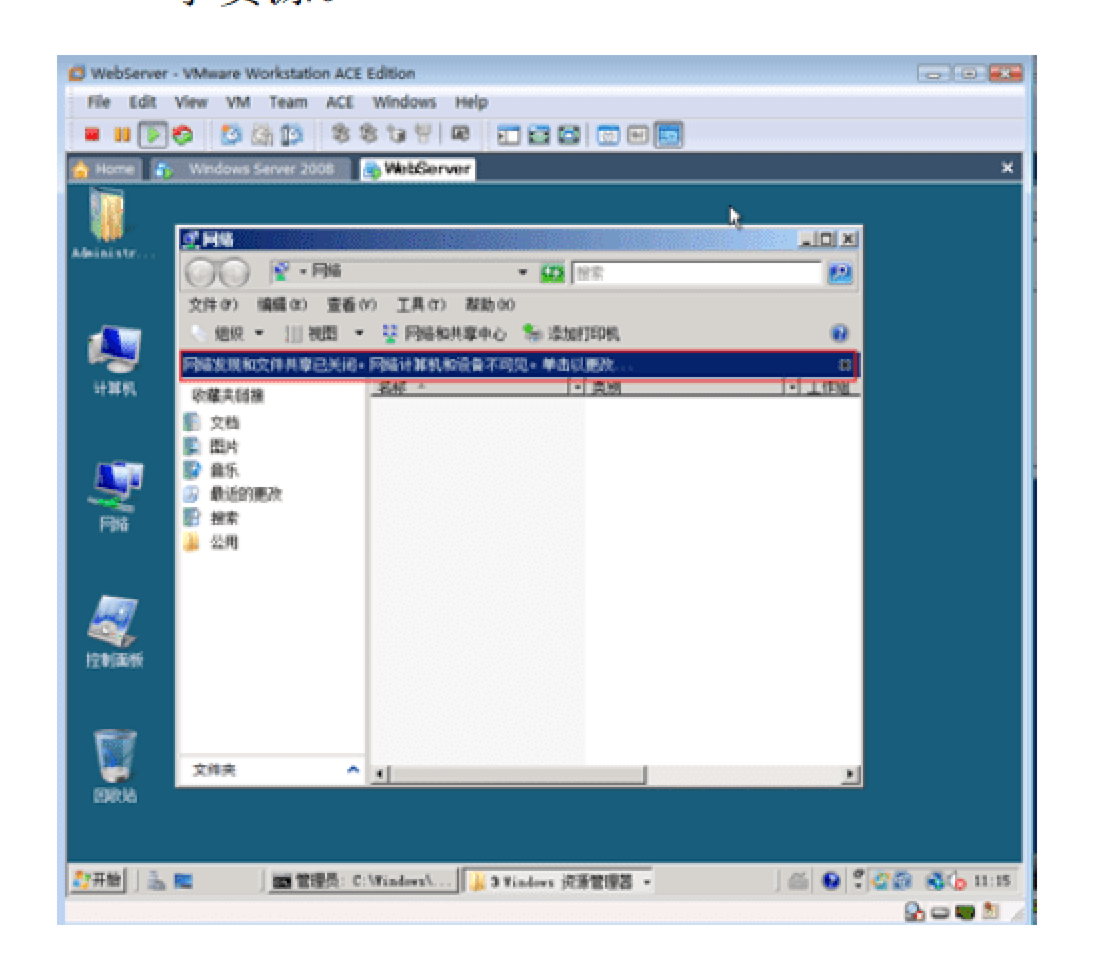


图 3-71　不能访问网络资源

图 3-72　访问网络资源失败

⑤　在 WebServer 上，单击“自定义”按钮，位置类型选中“专用”，单击“下一步”按钮，单击“完成”按钮，如图 3-73 所示。

⑥　如图 3-74 所示，注意观察，“网络发现”、“文件共享”已经启用。

⑦　如图 3-75 所示，再次打开网络，可以看到网络中的计算机，同时网络中的计算机也能看到这台计算机。

⑧　在 Windows Server 2008 上，如图 3-76 所示，再次 ping 10.7.10.102 发现能够返回数据包，先输入\\10.7.10.102，再输入 WebServer 上的账号和密码，发现能够访问其共享资源。

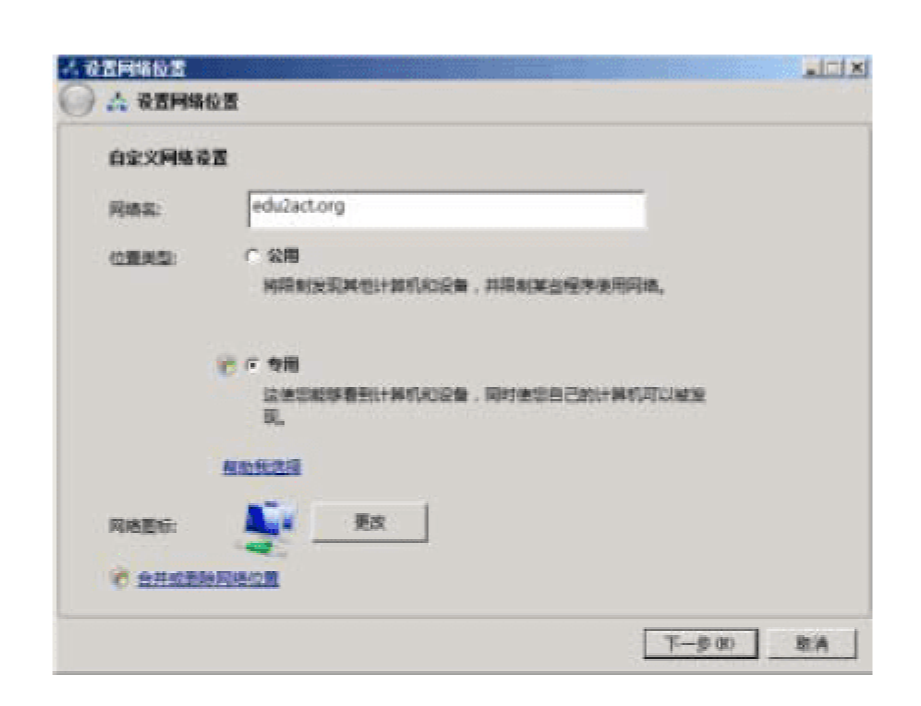


图 3-73　改变网络位置



图 3-74　启用“网络发现”和“文件共享”

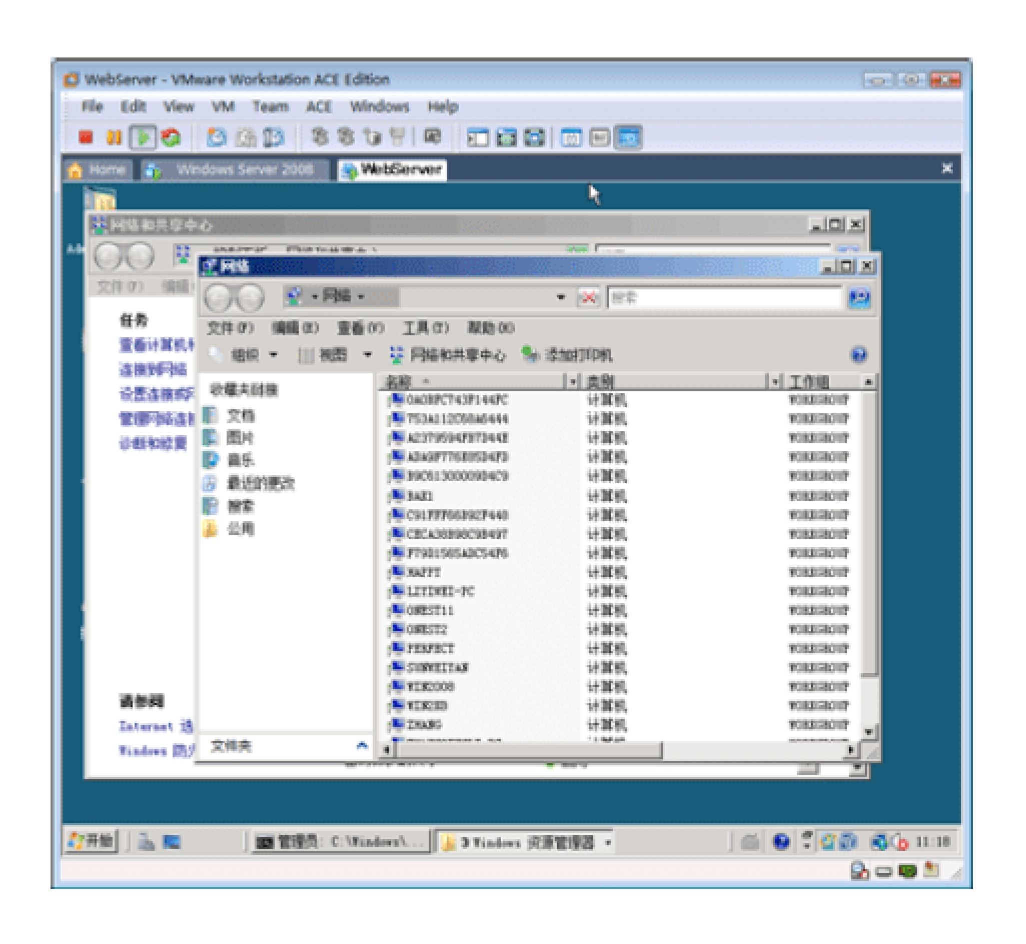


图 3-75　启用网络发现后浏览网上邻居

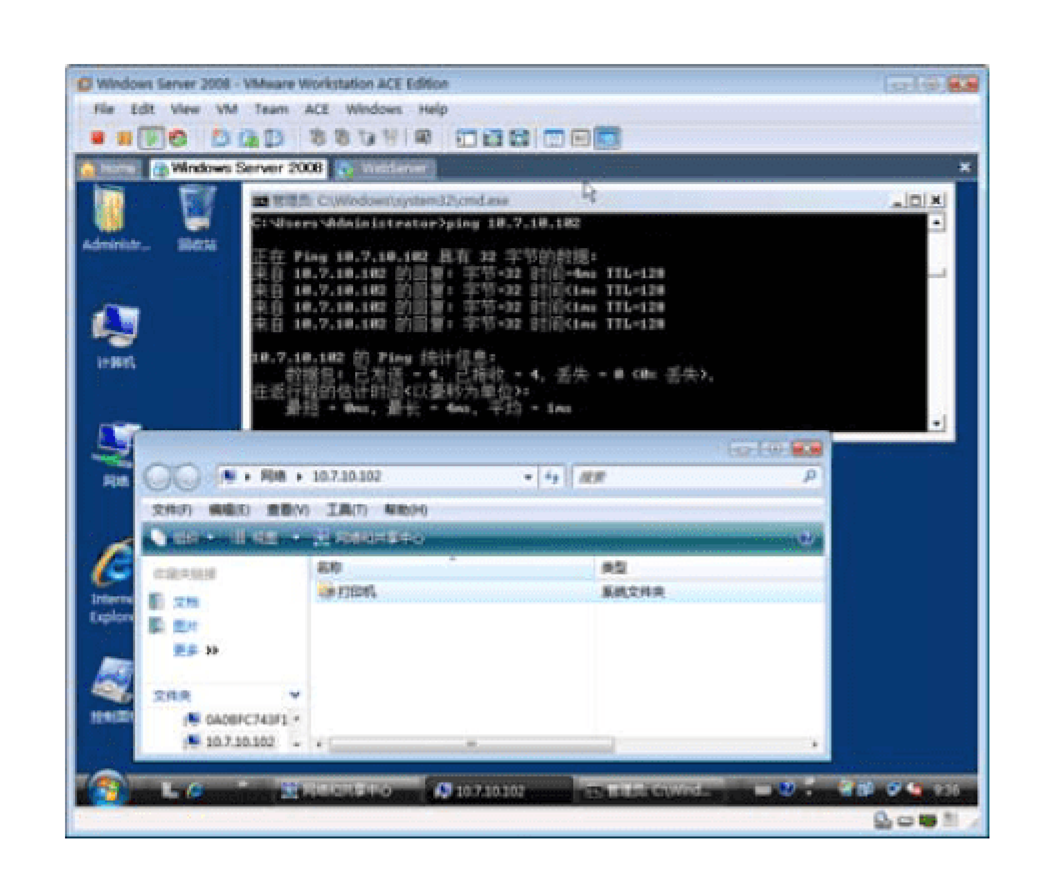


图 3-76　可以访问共享资源

3.8.3　任务 2：启用公用文件夹共享

任务描述

能够在专用网络位置启用公用文件夹共享，进一步理解网络位置的作用，了解公共文件夹的位置以及共享权限的设置。

实战环境

- Windows Server 2008 企业版操作系统 Windows Server 2008，IP 地址 10.7.10.114。
- Windows Server 2008 企业版操作系统 WebServer，IP 地址 10.7.10.102。

实战目标

- 在 WebServer 上的专用网络位置上启用公用共享文件夹。
- 能够知道公用文件夹所处的位置。

- 在 Windows Server 2008 上测试访问 WebServer 服务器上共享的公用文件夹。
- 更改 WebServer 上网络位置，快速切换网络安全配置。

实战步骤如下。

① 在 WebServer 上，打开“网络和共享中心”窗口，如图 3-77 所示，在“公用文件夹共享”右侧，单击▼按钮，选中“启用共享，以便能够访问网络的任何人都可以打开、更改和创建文件”复选框。

② 打开 C:\users 目录，可以看到“公用”文件夹已经为共享，如图 3-78 所示。

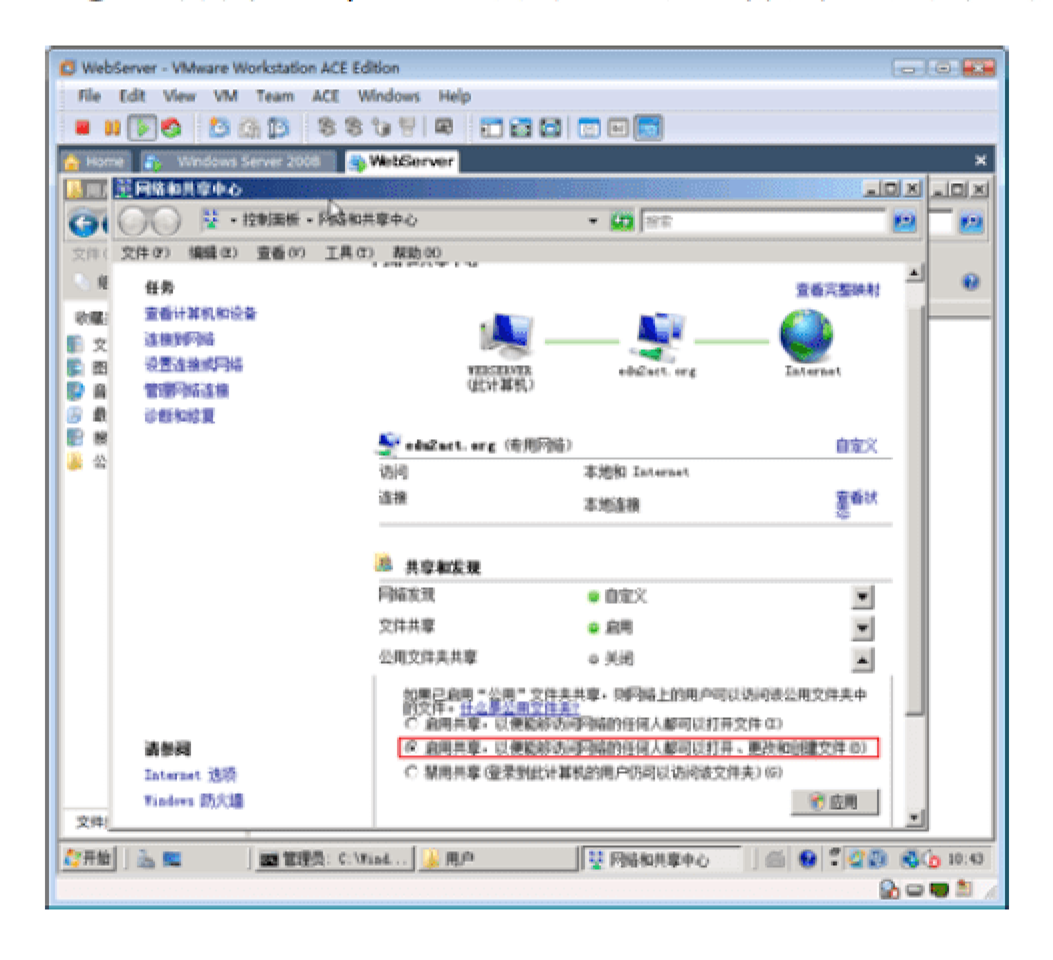


图 3-77　启用公用文件夹共享

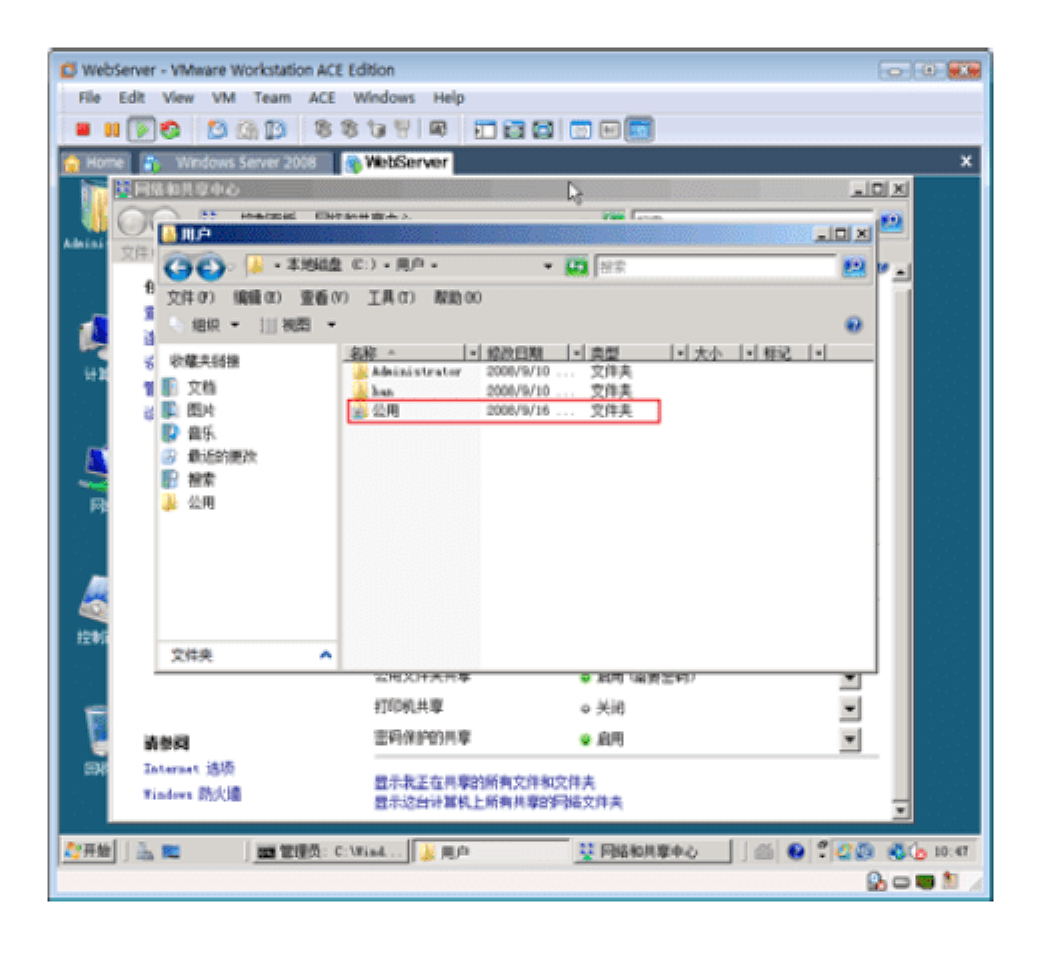


图 3-78　查看共享的公用文件夹

③ 在 Windows Server 2008 上，如图 3-79 所示，访问 10.7.10.102 共享文件夹，可以看到共享的文件夹 public。

④ 如果计算机在网吧或其他公共位置，不应该让其他计算机访问你的共享文件夹和其他的共享资源，则需要将网络位置设置成“公用”，如图 3-80 所示。可见网络位置可以让你快速切换网络安全的配置。

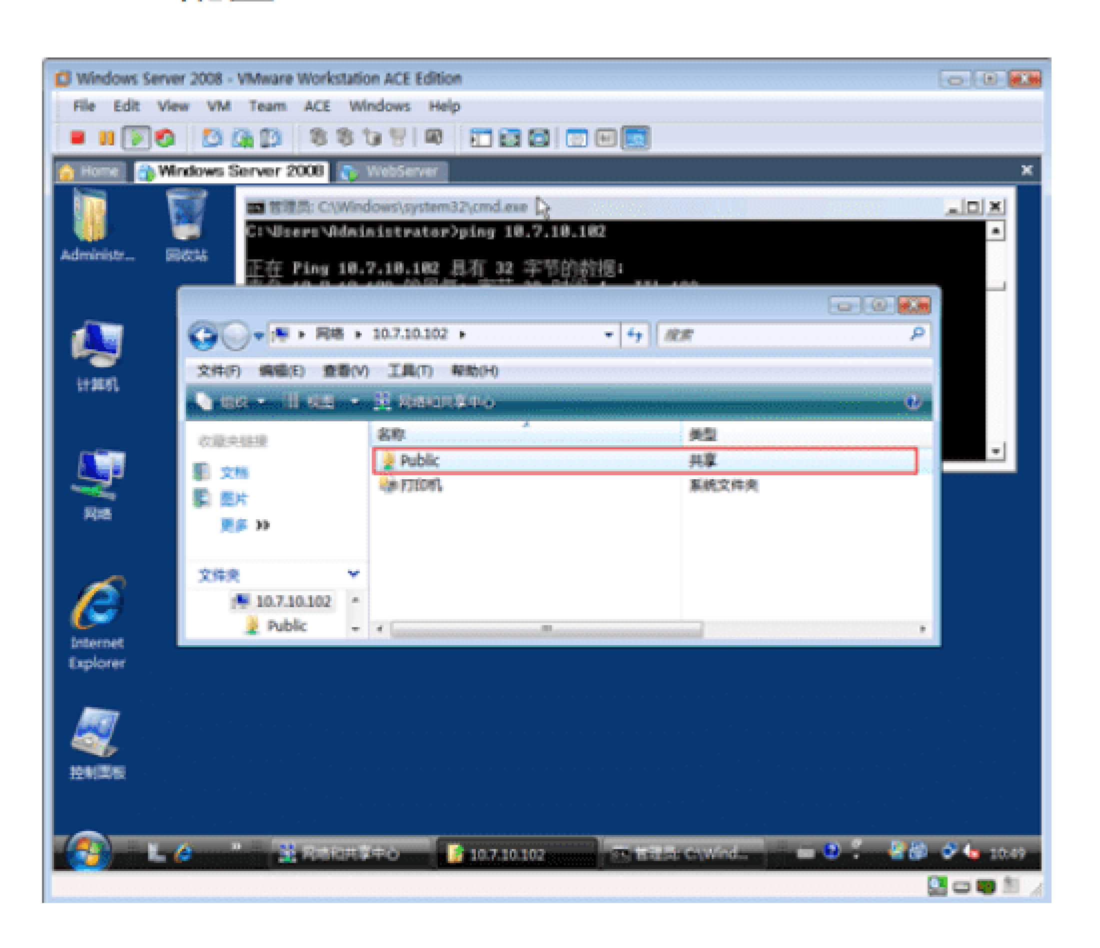




图 3-79　访问共享文件夹



图 3-80　更改网络位置为“公用”

⑤ 此时，在 Windows Server 2008 服务器上，将不能访问 WebServer 服务器上的共享资源。

3.9 实战 5：配置本地连接

任务描述

设置本地连接，使其直接使用 TCP/IPv4 进行通信；能够配置计算机使用动态 IP 地址、静态 IP 地址和备用地址；能够给计算机添加多个 IP 地址。

能够设置本地连接的 IP 配置和查看 IP 配置，能够测试网络连接。

实战环境

- Windows Server 2008 企业版操作系统 Windows Server 2008，IP 地址 10.7.10.114。
- Windows Server 2008 企业版操作系统 WebServer，IP 地址 10.7.10.102。
- 网络中有 DHCP 服务器。

实战目标

- 配置本地连接优先使用 IPv4 进行通信。
- 了解静态 IP 地址和动态 IP 地址。
- 能够配置本地连接的备用配置。
- 给本地连接指定静态 IP。
- 给本地连接指定多个 IP 地址和网管以及多个 DNS 服务器。
- 查看 IP 配置。
- 能够测试网络连接。
- 能够使用 ping 命令和 ipconfig 命令。

3.9.1 任务 1：配置本地连接直接使用 IPv4 进行通信

细心的朋友可能会感觉到，在 Windows Server 2008 系统环境下无论是上网访问还是进行共享传输，网络速度都没有以前那样一气呵成的感觉，好像总要比平时慢半拍似的，这是什么原因呢？



提示： 按理说，Windows Server 2008 系统在网络连接方面的功能应该更加强大，网络传输速度应该更快才对。其实这种现象是由于 Windows Server 2008 系统新增加了 TCP/IPv6 通信协议引起的。在上网访问或共享传输时，Windows Server 2008 系统在默认状态下会优先使用 TCP/IPv6 通信协议进行网络连接，而目前对应 TCP/IPv6 通信协议的网络连接是无效的，因为许多网络设备还不支持该协议进行通信，在发现使用 TCP/IPv6 协议通信失败后，系统会尝试使用 TCP/IPv4 协议进行通信，很显然 Windows Server 2008 系统的网络连接过程比以前多走了一些弯路，从而导致了网络传输速度比平时慢半拍。

要想使网络连接速度恢复到以前的水平，只需按照如下步骤操作，取消 TCP/IPv6 协议的选中状态，以便让 Windows Server 2008 系统直接使用 TCP/IPv4 协议进行通信传输。

① 在 WebServer 上，如图 3-81 所示，打开“网络和共享中心”窗口，单击“管理网络连接”按钮。

② 在“网络连接”窗口，双击“本地连接”图标，打开“本地连接 属性”对话框，如图 3-82 所示。此时会看到系统在默认状态下已经自动选中了“Internet 协议版本 6(TCP/IPv6)”复选框，这样的

话 Windows Server 2008 系统就会优先使用 TCP/IPv6 协议进行网络连接；为了让 Windows Server 2008 系统能够自动使用 TCP/IPv4 协议进行网络连接，需要取消选中“Internet 协议版本 6(TCP/IPv6)”复选框，同时保证“Internet 协议版本 4(TCP/IPv4)”选项与“Microsoft 网络的文件和打印机共享”选项处于选中状态，最后单击“确定”按钮，这样一来 Windows Server 2008 系统的网络连接速度就能恢复正常了。

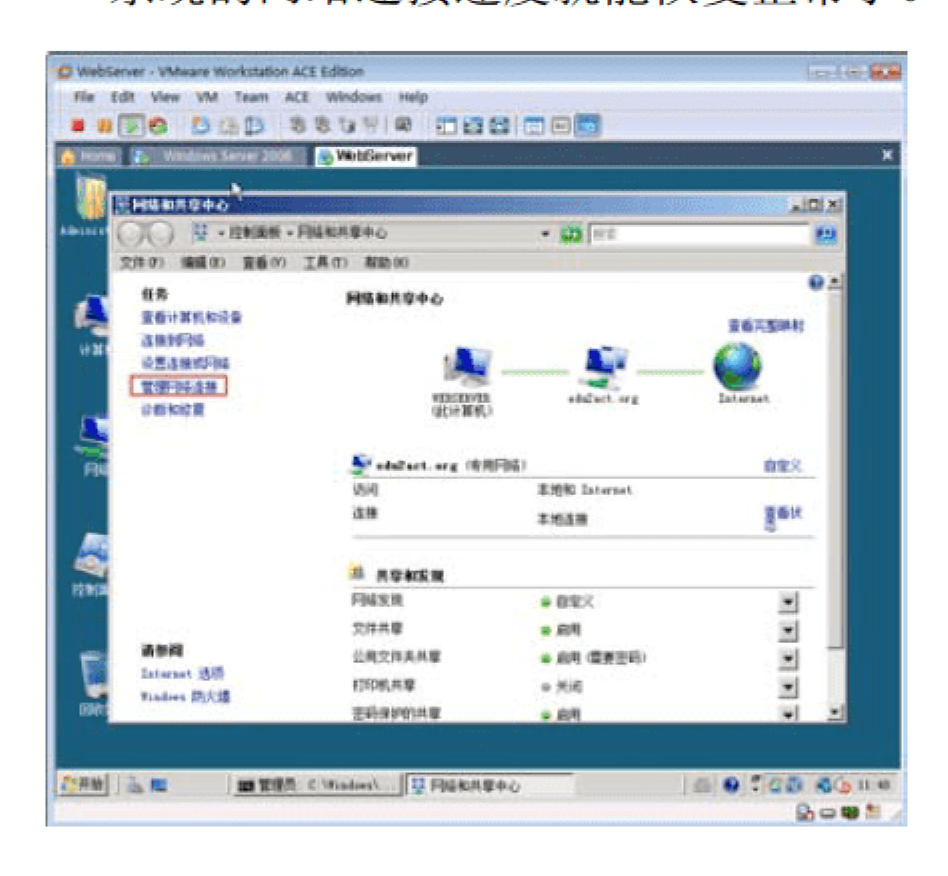


图 3-81　打开管理网络连接

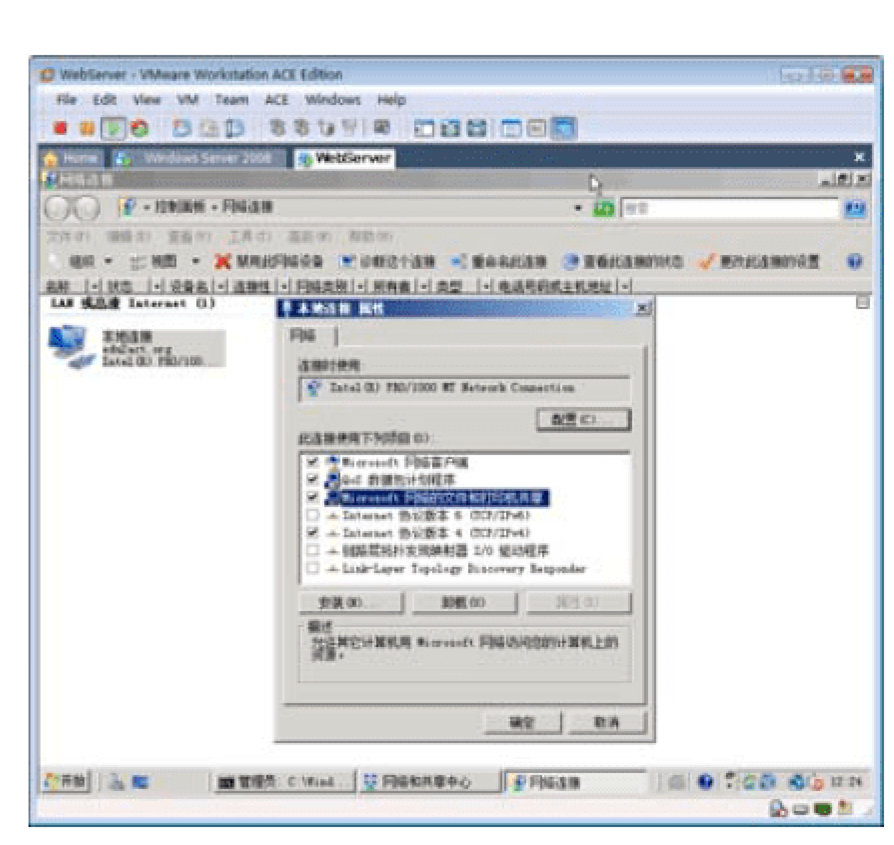


图 3-82　去掉 IPv6 选择

3.9.2　任务 2：配置 IP 地址

设置计算机 IP 地址有两种方式。

1. 动态 IP 地址

计算机有 DHCP 服务器分配地址。使用于网络规模大或计算机移动较为频繁的网络，这种方式有以下优点。

- 安全而可靠的设置：DHCP 避免了因手工设置 IP 地址及子网掩码所产生的错误，同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突。
- 降低了管理 IP 地址设置的负担：使用 DHCP 服务器大大缩短了配置或重新配置网络中工作站所花费的时间，而且通过对 DHCP 服务器的设置可灵活地设置 IP 地址的租期。同时，DHCP 地址租约的更新过程将有助于用户确定哪些客户的设置需要经常更新，且这些变更由客户机与 DHCP 服务器自动完成，无须网络管理员干涉。
- 使用自动专用 IP 寻址(APIPA)：在没有 DHCP 服务器的情况下为 DHCP 客户端提供 IP 地址，地址范围是从 169.254.0.1～169.254.255.254。比如当客户端在启动时与本地 DHCP 服务器通讯失败，无法更新它的租用时，它将使用 APIPA 分配的地址，以后每隔 5 min 尝试与外界的 DHCP 服务器联系一次，直到它可以与 DHCP 服务器通讯为止。

2. 静态 IP 地址

静态 IP 地址就是管理员指定的固定计算机的 IP 地址。在网络规模不大且网络中的计算机较为固定的情况下使用静态地址。

3. 配置动态 IP 和备用地址

① 在 WebServer 上，打开网络中心，单击“管理网络连接”按钮。

② 打开“网络连接”窗口，双击“本地连接”图标，如图 3-83 所示。在“本地连接 状态”对话框中，单击“属性”按钮。在“本地连接 属性”对话框中，选中“Internet 协议版本 4(TCP/IPv4)”复选框，单击“属性”按钮，打开如图 3-84 所示的对话框。

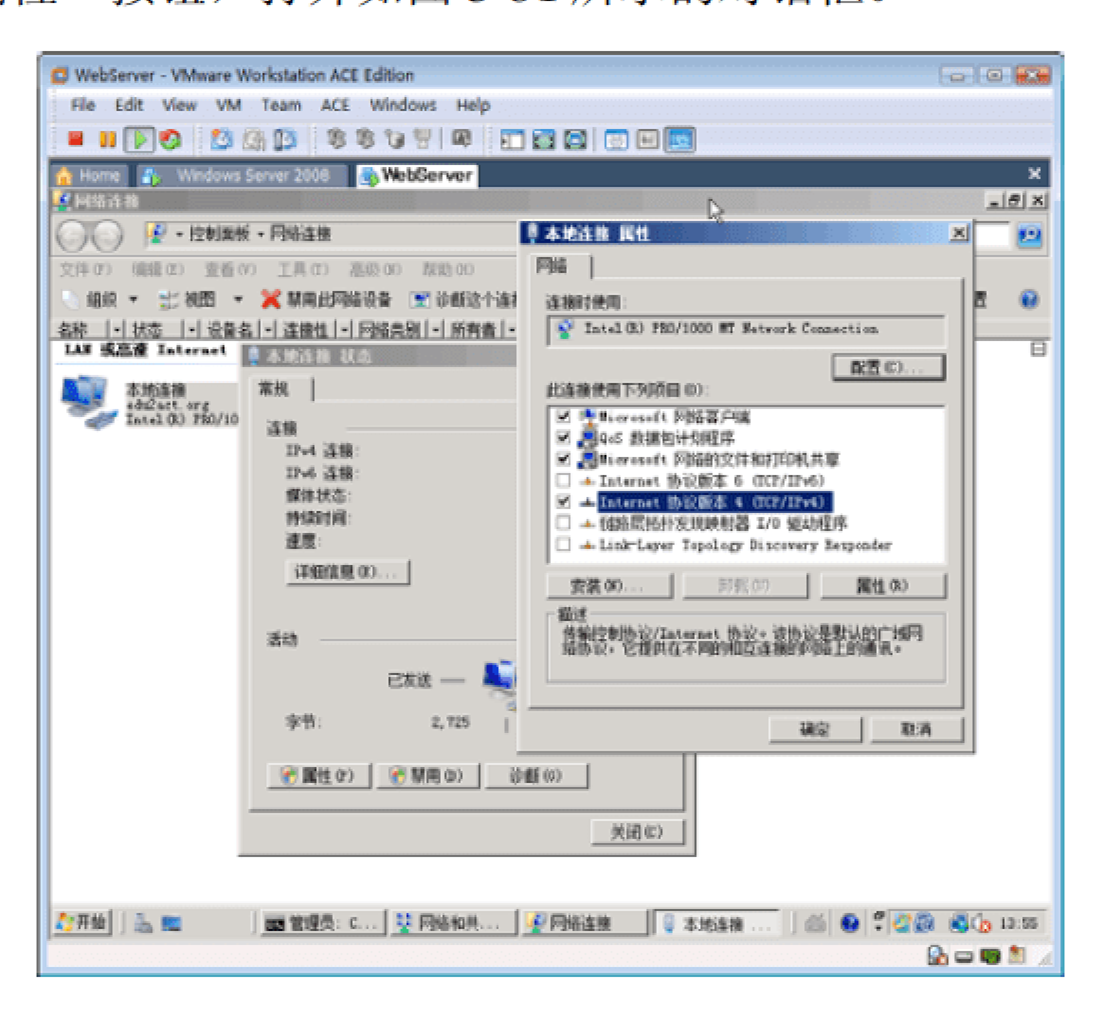


图 3-83　配置 TCP/IP 属性

③ 如图 3-84 所示，切换到“常规”选项卡，选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮。

④ 如图 3-85 所示，切换到“备用配置”选项卡，用户可以输入一个指定的备用地址。如果计算机从网络上没有获得 IP 地址，将会使用备用配置中指定的 IP 地址，而不是使用自动专用 IP 寻址(APIPA)。

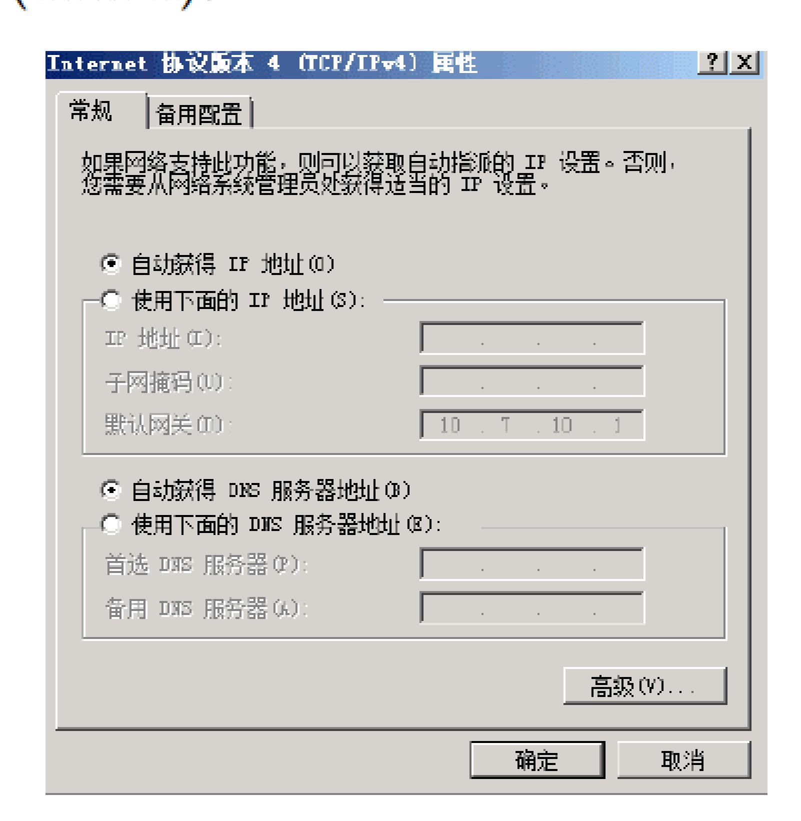


图 3-84　自动获得 IP 地址

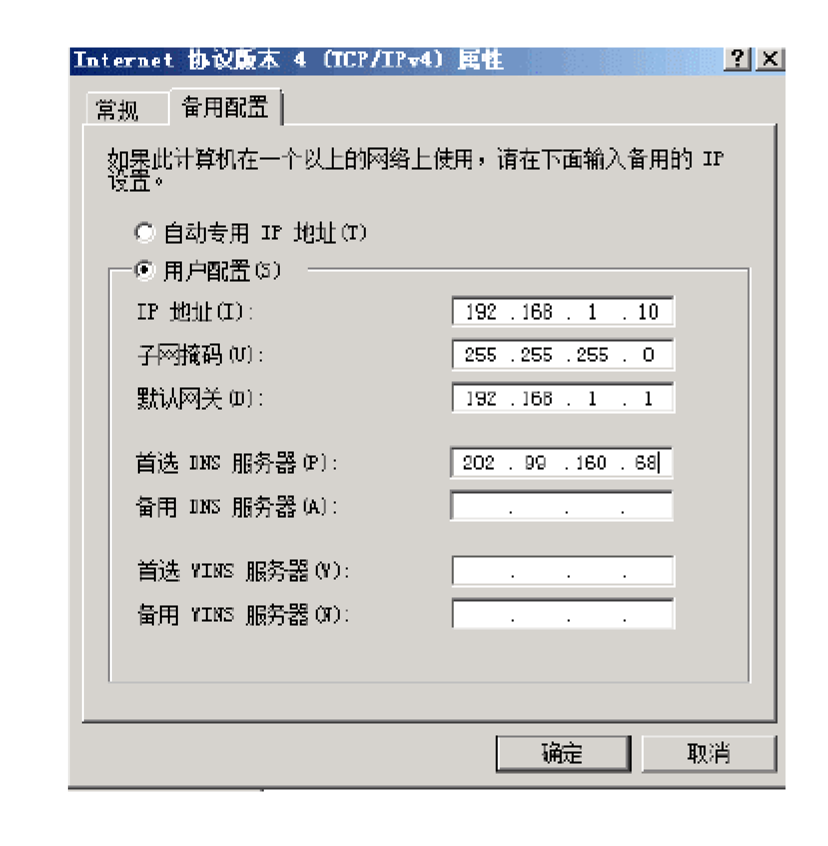


图 3-85　配置备用配置

⑤ 如图 3-86 所示，在“本地连接 状态”对话框中，单击“详细信息”按钮。

⑥ 如图 3-87 所示，可以看到从 DHCP 服务器获得的 IP 地址、子网掩码、网关，以及 DNS 服务器的地址、租约过期时间、DHCP 服务器信息。

⑦　如图 3-88 所示，在命令行输入 ipconfig /all，也可以显示 IP 配置。

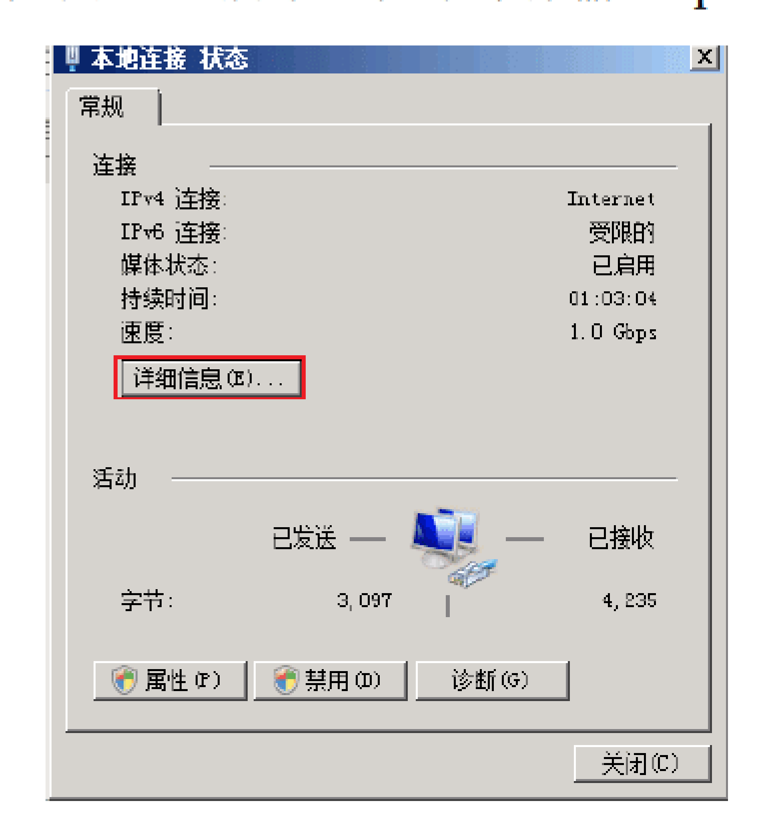



图 3-86　查看详细配置

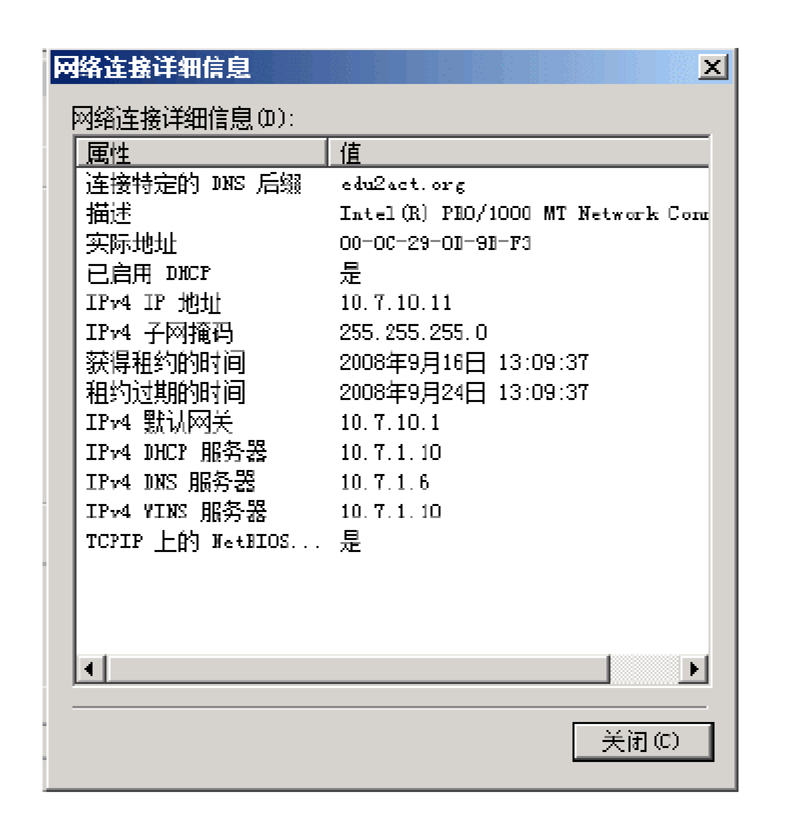


图 3-87　查看获得的 IP 配置

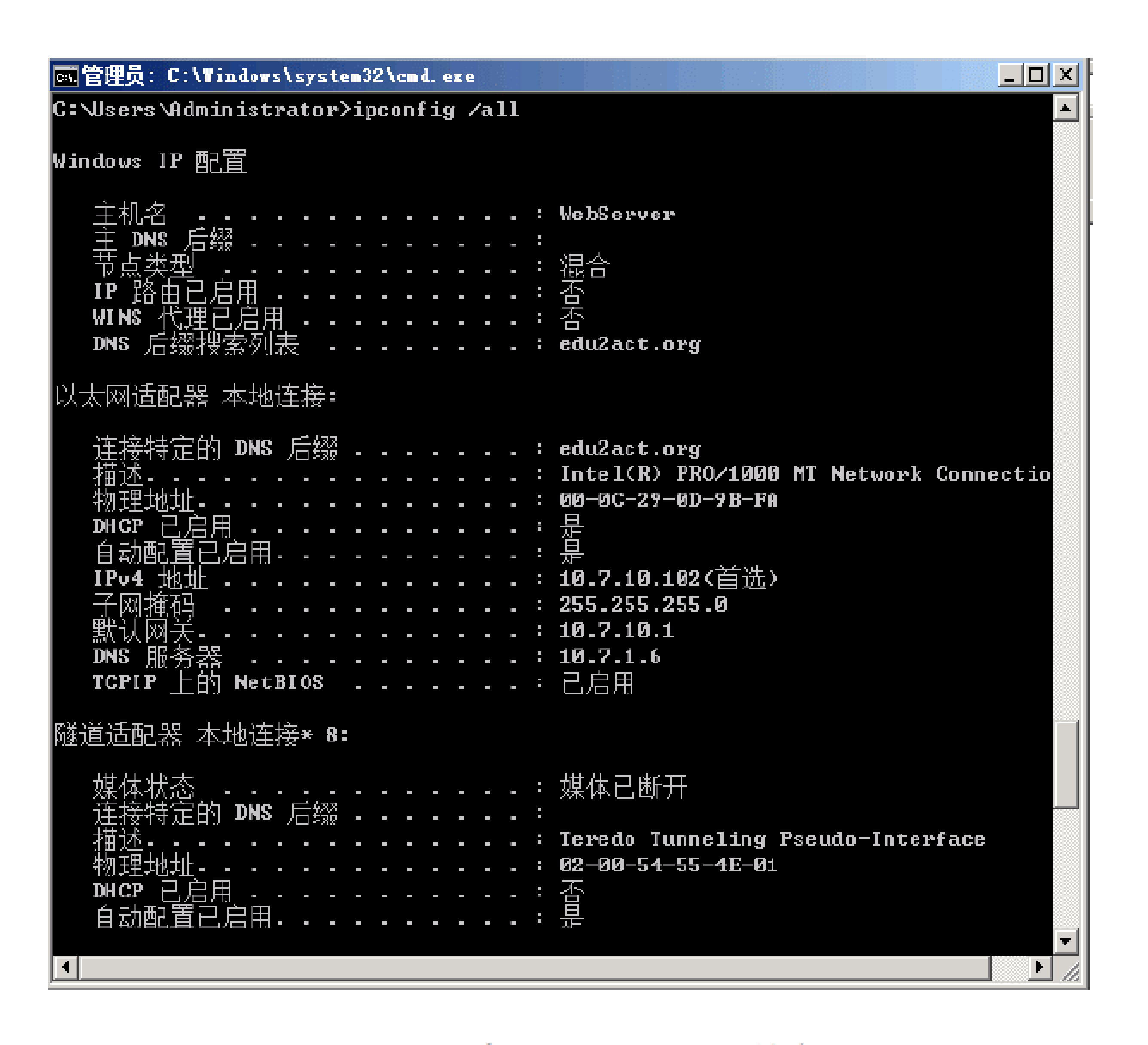


图 3-88　查看 TCP/IP 配置信息

4. 配置静态 IP 地址

①　打开“网络连接”窗口，双击“本地连接”图标，在“本地连接 状态”对话框中，单击“属性”按钮。在“本地连接 属性”对话框中，选中“Internet 协议版本 4(TCP/IPv4)”复选框，单击“属性”按钮。

②　如图 3-89 所示，在“Internet 协议版本 4(TCP/IPv4)属性”对话框中，选中“使用下面的 IP 地址”，输入静态 IP 地址、子网掩码、网关。选中“使用下面的 DNS 服务器地址”单选按钮，输入“首选 DNS 服务器”和“备用 DNS 服务器”的 IP 地址。

③　单击“高级”按钮，如图 3-90 所示，可以给计算机输入多个 IP 地址和网关。网关就是路由器的接口地址。如果你的网络到其他网段有多个出口，则可以添加多个网关来容错；如果你的网络就一个出口，默认网关指定一个。

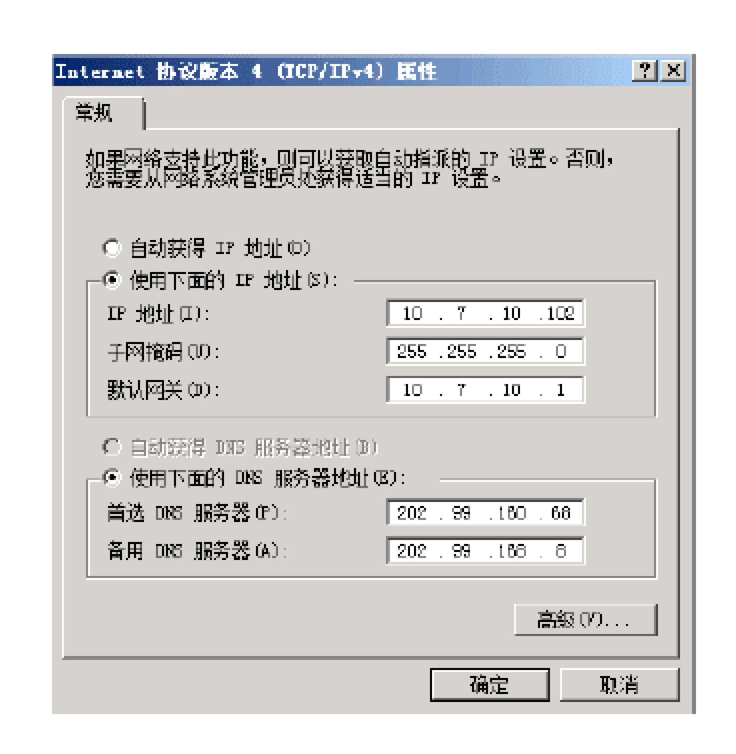


图 3-89　指定静态 IP 地址

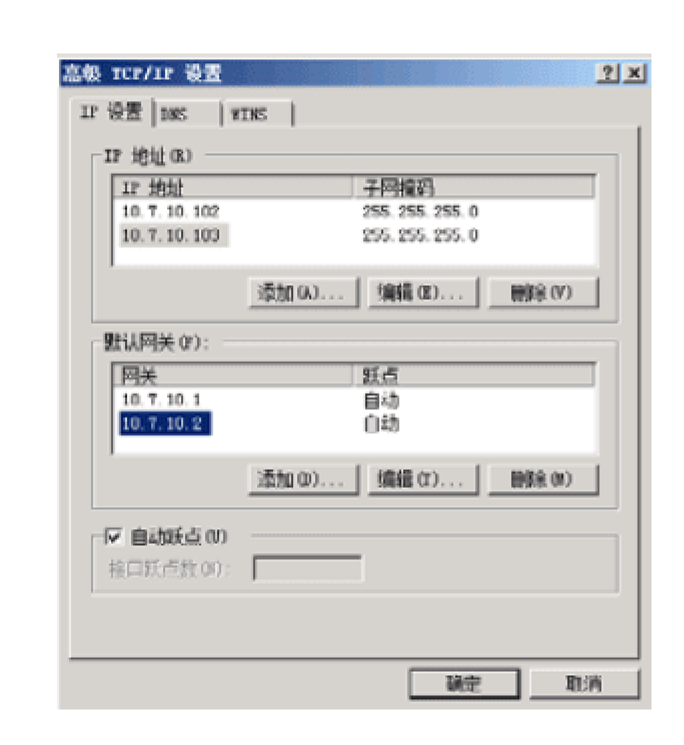


图 3-90　添加多个 IP 地址和网关

3.9.3　任务 3：更改计算机的 MAC 地址

MAC(Media Access Control，介质访问控制)地址是烧录在网卡(Network Interface Card，NIC)中的MAC 地址，也叫硬件地址，是由 48 b(6B)十六进制的数字组成。0～23 位，由厂家自己分配，24～47 位，叫做组织唯一标识符(organizationally unique)，是识别 LAN(局域网)节点的标识。其中第 40 位是组播地址标志位。网卡的物理地址通常是由网卡生产厂家烧入网卡的 EPROM(一种闪存芯片，通常可以通过程序擦写)，它存储的是传输数据时真正赖以标识发出数据的计算机和接收数据主机的地址。

也就是说，在网络底层的物理传输过程中，是通过物理地址来识别主机的，它一般也是全球唯一的。比如，著名的以太网卡，其物理地址是 48 b(比特位)的整数，如：44-45-53-54-00-00，以机器可读的方式存入主机接口中。以太网地址管理机构(除了管这个外还管别的)(IEEE，电气和电子工程师协会)将以太网地址，也就是 48 b 的不同组合，分为若干独立的连续地址组，生产以太网网卡的厂家就购买其中一组，具体生产时，逐个将唯一地址赋予以太网卡。

形象地说，MAC 地址就如同我们身份证上的身份证号码，具有全球唯一性。

有些防火墙是以客户端的 MAC 地址进行上网控制的，即使 MAC 地址在出厂时就已经固化在硬件中了，计算机也可以使用管理员指定的 MAC 地址来发送和接收数据帧。

查看和更改 MAC 地址

① 查看 IP 地址方法，在命令行中输入 ipconfig /all，如图 3-91 所示，在命令行中输入 getmac，如图 3-92 所示，均可显示网卡的 MAC 地址。

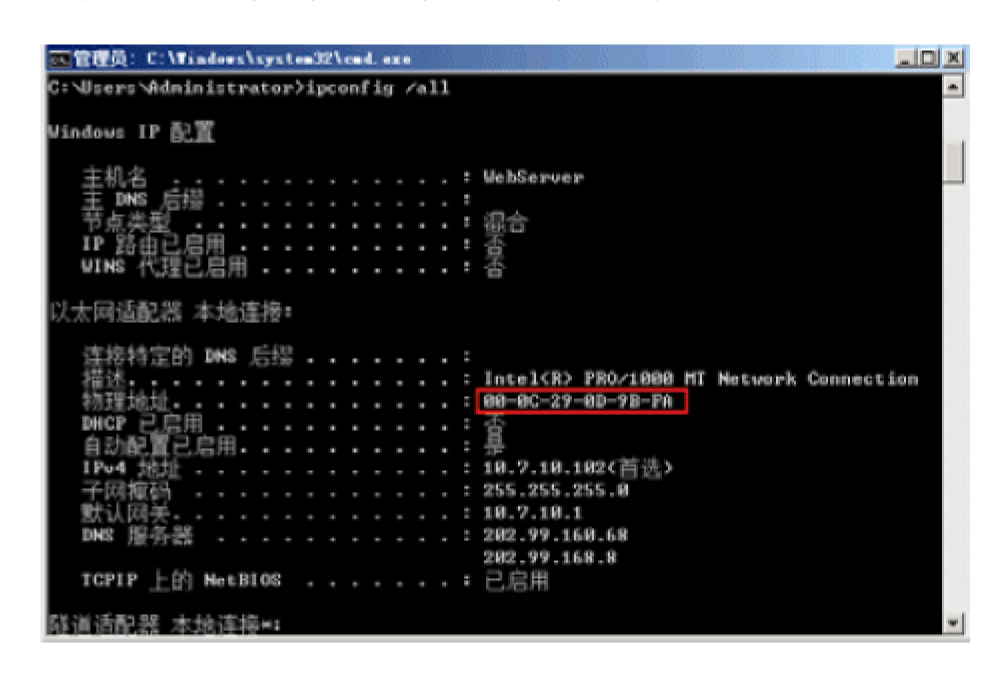


图 3-91　显示 MAC 地址(一)

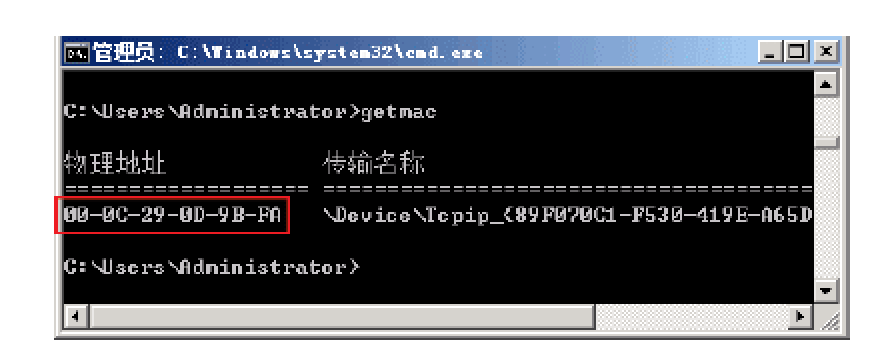


图 3-92　显示 MAC 地址(二)

② 如图 3-93 所示，在“本地连接 属性”对话框中，单击“配置”按钮。

③ 如图 3-94 所示，选中“本地管理地址”选项，输入新的 MAC 地址后。单击“确定”按钮。

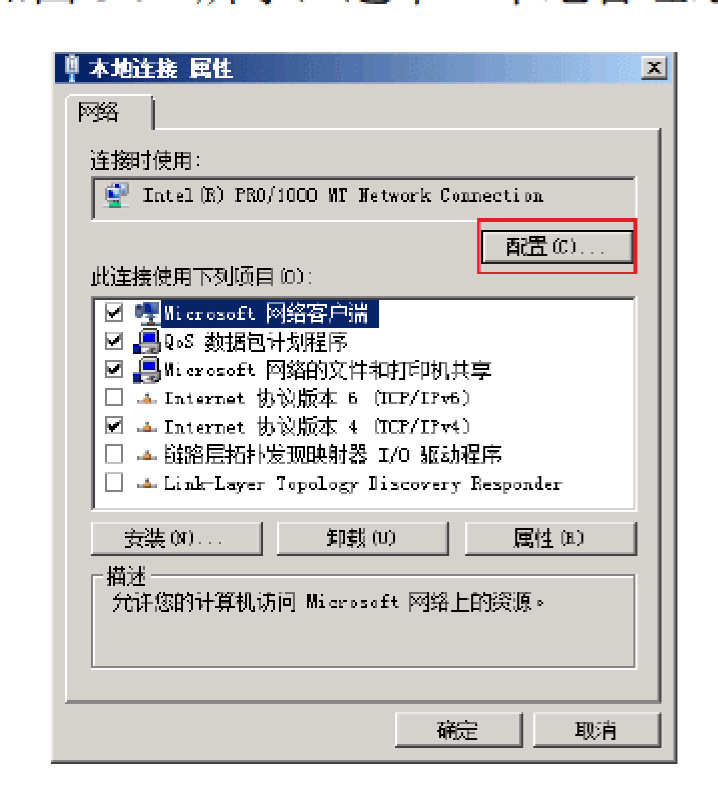




图 3-93　配置网络网卡



图 3-94　指定 MAC 地址

④ 再次查看 MAC 地址，输入 getmac，如图 3-95 所示。此时可发现已经是管理员指定的 MAC 地址了。计算机网卡上的 MAC 地址是不能更改的，只不过现在通信计算机使用管理员指定的 MAC 地址发送数据帧。

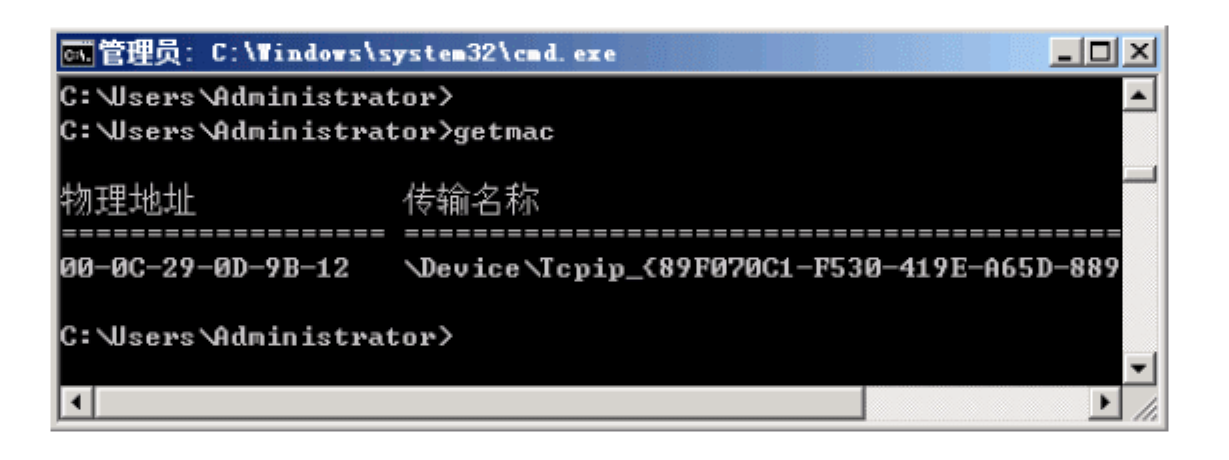


图 3-95　看到更改后的 MAC 地址

3.10　实战 6：常用网络排错工具

任务描述

能够学会使用常用网络排错工具进行网络故障诊断。

实战环境

- Windows Server 2008 企业版操作系统 Windows Server 2008。
- 能够访问 Internet。

实战目标

- 使用 ipconfig 检查本地连接配置。
- 使用 ping 测试网络连通性。
- 使用 pathping 跟踪数据包路径以了解网络状态。
- 使用 telnet 测试到远程计算机应用层的连接。
- 使用 netstat 检测网络状态。

3.10.1　任务 1：使用 ipconfig 确认 IP 地址配置正确

ipconfig 实用程序可用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。但是，如果你的计算机和所在的局域网使用了动态主机配置协议(Dynamic Host Configuration Protocol，DHCP——Windows NT 下的一种把较少的 IP 地址分配给较多主机使用的协议，类似于拨号上网的动态 IP 分配)，这个程序所显示的信息也许更加实用。这时，ipconfig 可以让你了解计算机是否成功地租用到一个 IP 地址，如果租用到，则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和默认网关实际上是进行测试和故障分析的必要项目。

在命令行输入 ipconfig/all，查看 IP 地址是否冲突。如图 3-96 所示，提示 IP 地址冲突，需要重新更改一个 IP 地址。



图 3-96　查看 IP 配置

3.10.2　任务 2：使用 ping 测试网络连通性

ping(Packet Internet Grope，因特网包探测器)是用于测试网络连接量的程序。ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。一般用于检测网络通与不通，也叫时延，其值越大，速度越慢。

它是用来检查网络是否通畅或者网络连接速度的命令。作为一个生活在网络上的管理员来说，ping 命令是第一个必须掌握的 DOS 命令，它所利用的原理是这样的：网络上的机器都有唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包我们可以确定目标主机的存在，可以初步判断目标主机的操作系统等。

ping 是 Windows 系列自带的一个可执行命令。利用它可以检查网络是否能够连通，用好它可以很好地帮助我们分析判定网络故障。应用格式：“ping IP 地址”。该命令还可以加许多参数使用，具体是：输入 ping，按 Enter 键即可看到详细说明。

ping 指的是端对端连通，通常用来作为可用性的检查，但是某些病毒木马会强行大量远程执行 ping

命令而抢占网络资源，从而导致系统变慢，网速变慢。严禁 ping 入侵作为大多数防火墙的一个基本功能提供给用户进行选择。

ping 本机 IP，如图 3-97 所示，本机 IP 地址为 10.7.10.102，如果出现来自 10.7.10.102 的回复，则表明网卡安装配置没有问题，IP 地址也不冲突；如果出现如图 3-98 所示的消息，则表明 IP 地址冲突。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 10.7.10.102

正在 Ping 10.7.10.102 具有 32 字节的数据:
来自 10.7.10.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.7.10.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.7.10.102 的回复: 字节=32 时间<1ms TTL=128
来自 10.7.10.102 的回复: 字节=32 时间<1ms TTL=128

10.7.10.102 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 0ms，平均 = 0ms

C:\Users\Administrator>_
```

图 3-97　IP 地址配置成功



图 3-98　IP 地址冲突的情况

如图 3-99 所示，ping 网关，能通，则表明局域网中的网关路由器在正常运行；反之，则说明网关有问题。局域网延迟一般在 1 ms，如果延迟持续大于 1 ms，则表明局域网有点堵塞。加参数 –t 就一直 ping 下去，按 Ctrl +C 组合键结束，否则测试 4 个包结束。



图 3-99　查看延迟和丢包率

ping 远程 IP，这一命令可以检测本机能否正常访问 Internet。比如本地电信运营商的 IP 地址为：202.99.160.68。如图 3-100 所示，可以看到到该地址的响应延迟为 68 ms，带宽比不上局域网。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 202.99.160.68

正在 Ping 202.99.160.68 具有 32 字节的数据:
来自 202.99.160.68 的回复: 字节=32 时间=69ms TTL=239
来自 202.99.160.68 的回复: 字节=32 时间=68ms TTL=239
来自 202.99.160.68 的回复: 字节=32 时间=68ms TTL=239
来自 202.99.160.68 的回复: 字节=32 时间=68ms TTL=239

202.99.160.68 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 68ms，最长 = 69ms，平均 = 68ms

C:\Users\Administrator>_
```

图 3-100　测试到 Internet 的连通性

ping 域名，这一命令测试你是否能够解析域名。如图 3-101 所示，ping www.inhe.net 能够解析出 IP 地址，并且还能够和这个 IP 地址连通。如果出现找不到主机，如图 3-102 所示，那就是域名解析出现问题，检查域名拼写是否正确，再就是更改计算机使用首选和备用的 DNS 服务器。

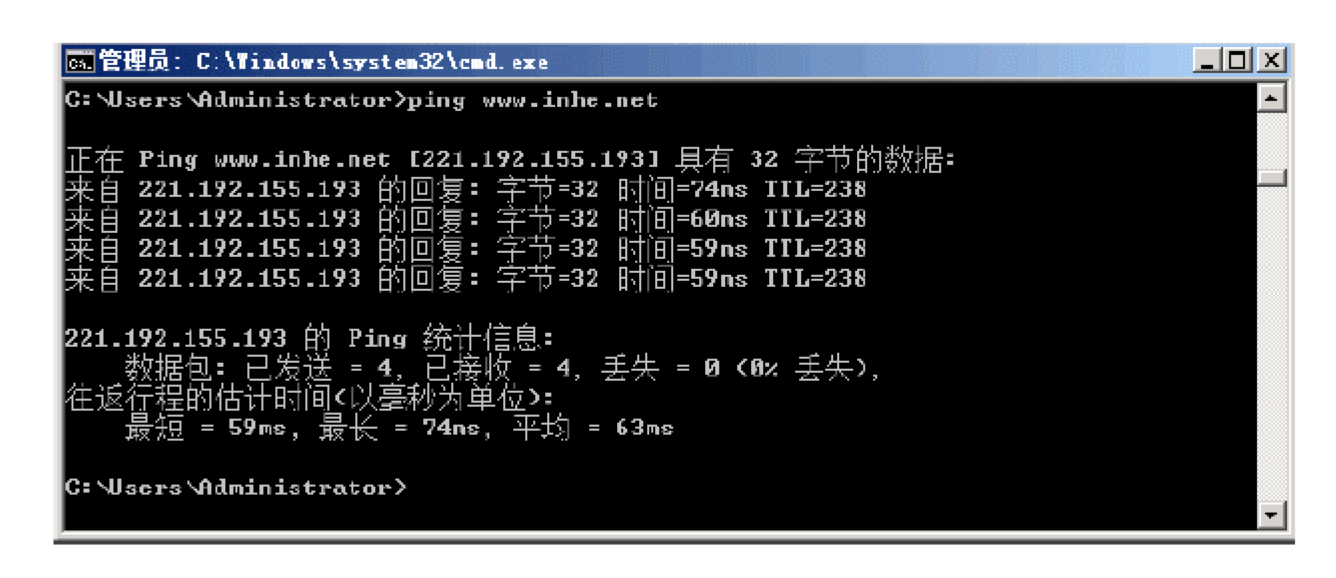


图 3-101　测试域名解析

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping www.baidu.com
Ping 请求找不到主机 www.baidu.com。请检查该名称，然后重试。

C:\Users\Administrator>
```

图 3-102　域名解析失败

3.10.3　任务 3：pathping 跟踪数据包的路径

pathping

提供有关在源和目标之间的中间跃点处网络滞后和网络丢失的信息。Pathping 在一段时间内将多个回响请求消息发送到源和目标之间的各个路由器，然后根据各个路由器返回的数据包计算结果。因为 pathping 显示在任何特定路由器或链接处的数据包的丢失程度，所以用户可据此确定存在网络问题的路由器或子网。pathping 通过识别路径上的路由器来执行与 tracert 命令相同的功能。然后，该命令在一段指定的时间内定期将 ping 命令发送到所有的路由器，并根据每个路由器的返回数值生成统计结果。如果不指定参数，pathping 则显示帮助。

```
C:\pathping 10.54.1.196
Tracing route to server1 [10.54.1.196]
over a maximum of 30 hops:
 0  172.16.87.35
 1  172.16.87.218
 2  192.168.52.1
 3  192.168.80.1
 4  10.54.247.14
 5  10.54.1.196
Computing statistics for 125 seconds...
Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
 0                                172.16.87.35
                  0/ 100 =  0%   |
1   41ms    0/ 100 =  0%     0/ 100 =  0%  172.16.87.218
                 13/ 100 = 13%   |
2   22ms   16/ 100 = 16%     3/ 100 =  3%  192.168.52.1
                  0/ 100 =  0%   |
3   24ms   13/ 100 = 13%     0/ 100 =  0%  192.168.80.1
                  0/ 100 =  0%   |
4   21ms   14/ 100 = 14%     1/ 100 =  1%  10.54.247.14
                  0/ 100 =  0%   |
5   24ms   13/ 100 = 13%     0/ 100 =  0%  10.54.1.196
Trace complete.
```

图 3-103　路径跟踪和丢包率

如果运行 pathping，如图 3-103 所示，在测试问题时首先将看到路由的结果。此路径与 tracert 命令所显示的路径相同。然后 pathping 命令将在下一个 125 ms 内显示忙消息(此时间根据跃点计数变化)。在此期间，pathping 从以前列出的所有路由器和它们之间的链接之间收集信息。在此期间结束时，显示测试结果。

最下边的两行 This Node/Link 和 Lost/Sent=Pct Address 包含最有用的信息。172.16.87.218(跃点 1)和 192.168.52.1(跃点 2)丢失 13%的数据包。所有其他链接工作正常。在跃点 2 和 4 处的路由器也丢失了传送给它们的数据包(如 This Node/Link 列中所示)，但是该丢失不会影响它们的转发路径。

对链接显示的丢失率(在最右边的栏中标记为 |)表明沿路径转发所丢失的数据包。该丢失表明链接阻塞。对路由器显示的丢失率(通过最右边栏中的 IP 地址显示)表明这些路由器的 CPU 可能超负荷运行。这

些阻塞的路由器可能也是端对端问题的一个因素，尤其是在软件路由器转发数据包时。

3.10.4　任务 4：使用 telnet 检查 TCP 会话建立情况

要验证使用已知的目标 TCP 端口号是否能建立 TCP 连接，可以使用 telnet IPv4Address TCPPort 命令。例如，要验证 IPv4 地址为 131.107.78.12 计算机上的 Web 服务器服务是否正在接受 TCP 连接，应使用 telnet 131.107.78.12 80 命令。

如果 telnet 工具成功地创建了 TCP 连接，命令提示窗口将会清空，然后根据协议显示一些文本。此窗口允许你针对已连接的服务输入命令。输入 Control-C，退出 telnet 工具。如果 telnet 工具无法成功创建 TCP 连接，将显示消息“正在连接到 IPv4Address...不能打开到主机的连接，端口为 TCPPort: 连接失败”。

如果使用 IE 浏览器不能打开 www.inhe.net 网站，而不能确定是 IE 浏览器配置出现了问题还是中了恶意插件造成的。则需要使用 telnet www.inhe.net 80 来检查是否能够使用 TCP 80 端口与 www.inhe.net 网站建立会话。如果使用 telnet 能够建立会话，则说明是 IE 浏览器配置引起的问题，如果提示打开 80 端口失败，那就是网络问题引起的，应该检查防火墙是否过滤掉了 TCP 80 数据包。

在 Windows Server 2008 中需要添加 Windows Server 功能中的 telnet 客户端，才能使用 telnet 命令。如图 3-104 所示。

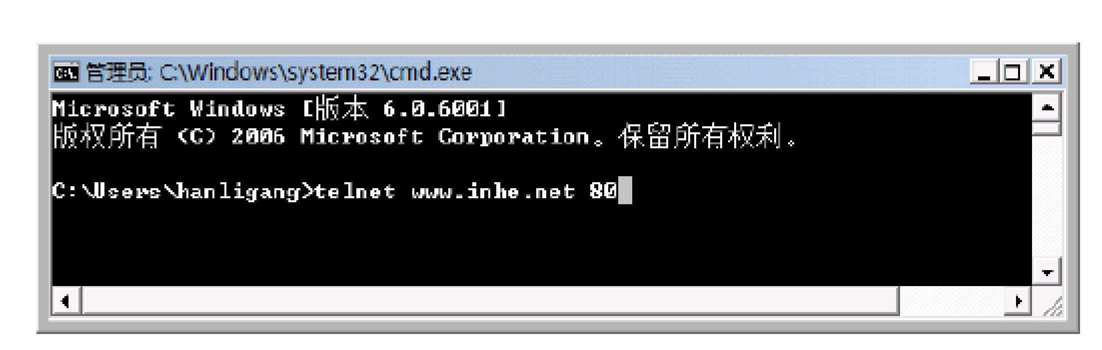


图 3-104　测试能否访问银河网站的 80 端口

如果 telnet 工具成功地创建了 TCP 连接，命令提示窗口将会清空；否则将会提示在 80 端口连接失败。如图 3-105 所示，telnet www.inhe.net 21 端口失败，说明 www.inhe.net 服务器没有使用 TCP 21 端口侦听的服务。

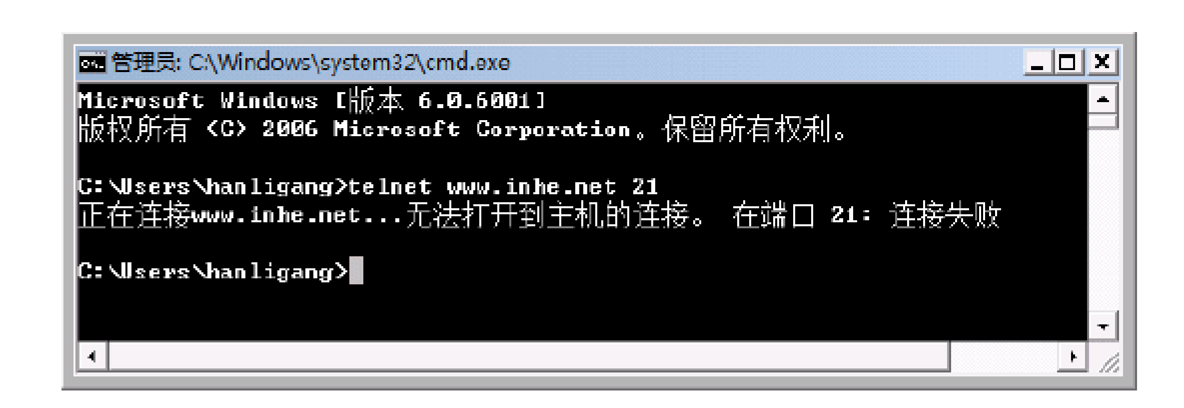


图 3-105　测试能否访问银河网站的 21 端口

3.10.5　任务 5：使用 netstat 检测网络状态

1. netstat

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运行。在命令行下输入 netstat /?，能够看到可用的参数。

```
C:\Users\hanligang>netstat /?
```

显示协议统计和当前 TCP/IP 网络连接。

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
```

其中的选项说明如下。

-a：显示所有连接和侦听端口。

-b：显示在创建每个连接或侦听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接或侦听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部[]中，它调用的组件位于顶部，直至达到 TCP/IP。注意，此选项可能很耗时，并且在你没有足够权限时可能失败。

-e：显示以太网统计。此选项可以与 -s 选项结合使用。

-f：显示外部地址的完全限定域名(FQDN)。

-n：以数字形式显示地址和端口号。

-o：显示拥有的与每个连接关联的进程 ID。

-p proto：显示 proto 指定的协议的连接。proto 可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起用来显示每个协议的统计，proto 可以是下列任何一个：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。

-r：显示路由表。

-s：显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计；-p 选项可用于指定默认的子网。

-t：显示当前连接卸载状态。

interval：重新显示选定的统计，各个显示间暂停的间隔秒数。按 Ctrl+C 组合键停止重新显示统计。如果省略，则 netstat 将打印当前的配置信息一次。

2. 使用 netstat 查看本地计算机侦听的端口

某家公司的网站不能访问了，操作系统是 Windows 2003。打开发现该 Web 站点停止，启动服务出现如图 3-106 所示的错误。

这台服务器上就一个 Web 站点，则肯定是其他程序占用了该 Web 站点使用的 80 端口，如何确认哪个程序占用该端口了呢？

① 在命令提示符下输入 netstat –aonb >>c:\p.txt，这样就把输出结果保存在 c:\p.txt 记事本文件中了。

② 打开 C 盘根目录下 p.txt。

③ netstat –aonb 这个命令能够查看侦听的端口以及侦听端口的进程号和应用程序名称。如图 3-107 所示，发现是 Web 迅雷占用了 80 端口，造成服务器 Web 服务启动失败。

④ 使用 netstat 找到了占用 80 端口的进程，原来是在该服务器上安装了 Web 迅雷而占用了 TCP 的 80 端口，这与 Web 站点使用的端口冲突，所以 Web 站点启动失败。这个实例告诉我们，计算机上的网络服务必须使用独立的端口标识，如果冲突，后启动的服务将无法启动。

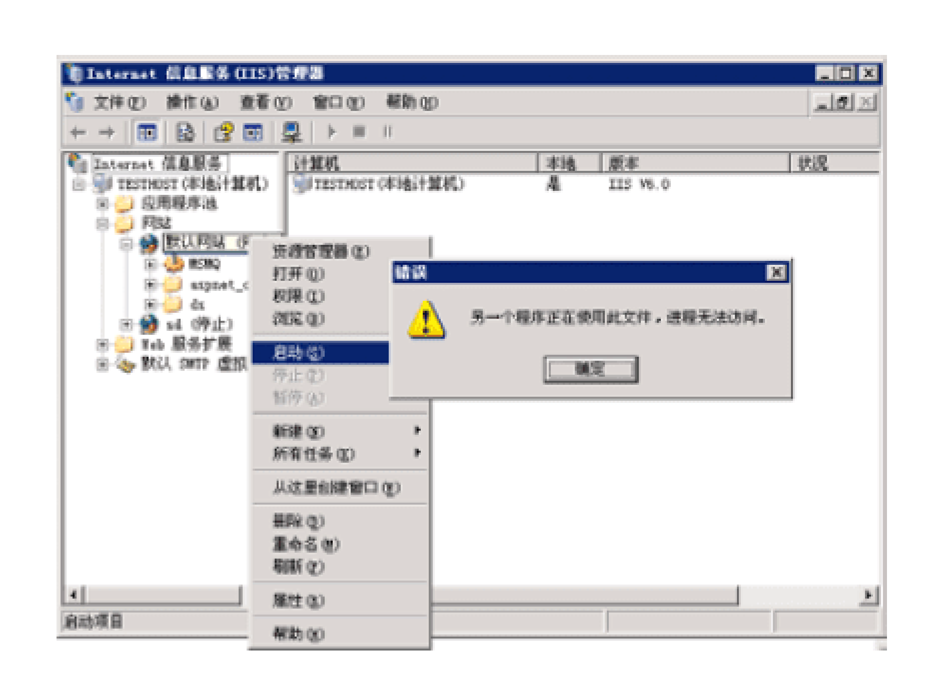


图 3-106　Web 服务启动失败

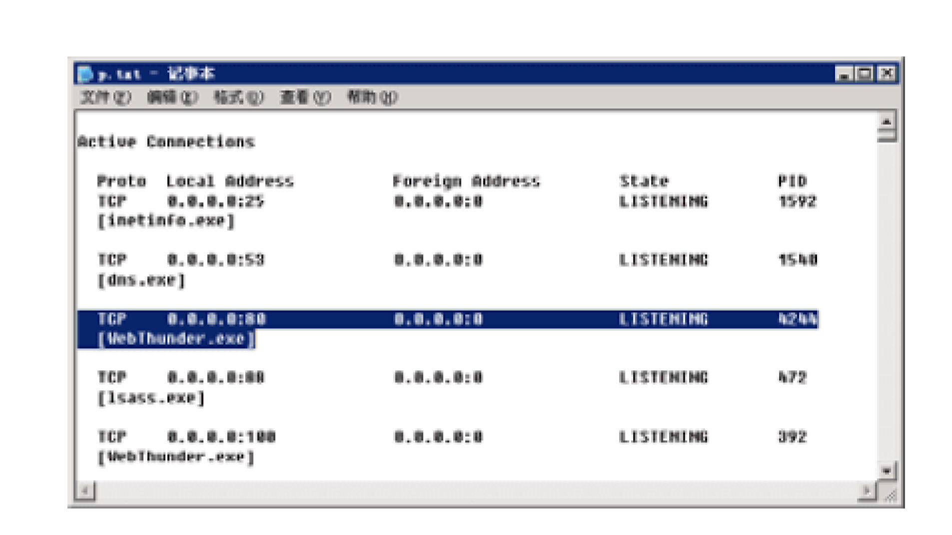


图 3-107　查看使用 80 端口的程序

3. 显示建立的会话查找木马

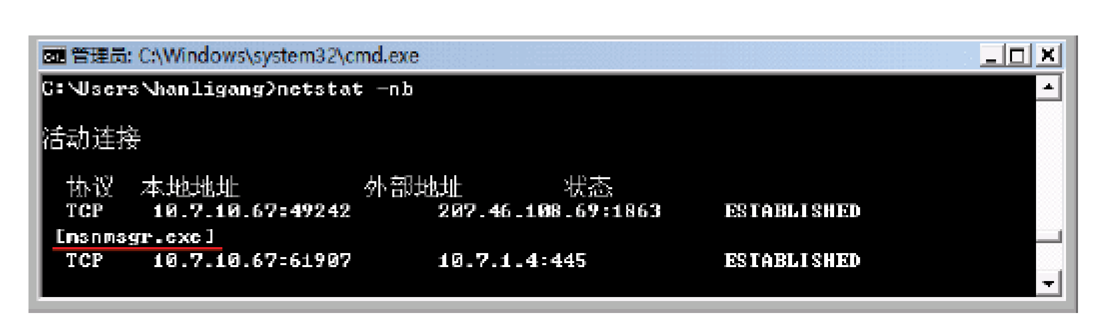
某单位的服务器最近出现异常，网管感觉有人在操作他的服务器，怀疑服务器中了木马。他想查一下服务器，如何确认服务器是否有木马？

若计算机中了木马，木马程序会自动运行，或者作为计算机上的一个服务或开机就自动运行的程序。然后就在后台偷偷地与远程的客户端连接。攻击者就可以使用客户端远程控制你的计算机。

如何确认是否中了木马程序？木马程序会自动与外网的客户端建立连接，可以查看计算机的对外连接，查找木马。

① 登录计算机，但不访问其他计算机，并且保证 Windows 没有在后台更新系统或杀毒软件没有更新病毒库，因为这些活动也会建立会话，干扰查找木马。

② 运行 netstat –nb，查看有没有到 Internet 上连接。如图 3-108 所示，只有 msnmsgr.exe 对外建立的会话，不过它不是木马。如果你觉得该进程可疑，可以访问 www.baidu.com，输入 msnmsgr 搜索，查看其是否为木马程序。



```
C:\Users\hanligang>netstat -nb

活动连接

  协议  本地地址          外部地址             状态
  TCP   10.7.10.67:49242  207.46.108.69:1863   ESTABLISHED
 [msnmsgr.exe]
  TCP   10.7.10.67:61907  10.7.1.4:445         ESTABLISHED
```

图 3-108　查看侦听端口程序

3.11　配置 Windows Server Core 环境

以管理员身份登录 Windows Server Core，将看到“命令提示符”窗口。

Server Core 没有图形界面，登录以后仅有一个“命令提示符”窗口。

在“命令提示符”窗口中，输入命令 prompt [$t]$spg，然后按 Enter 键。

此命令使得可以在命令提示符中显示时间。

输入 cd c:\windows\system32，然后按 Enter 键。

输入 cscript SCregEdit.wsf /cli，然后按 Enter 键。

SCregEdit.wsf 是 Server Core 特有的脚本，其中的 cli 开关非常有用，它可以把所有常见的配置 Server Core 的命令全部列出，而不需要管理员自己摸索。

输出结果。

```
Microsoft (R) Windows Script Host Version 5.7
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。
```

激活

```
Cscript slmgr.vbs -ato
```

使用 KMS 批量授权进行激活

配置 KMS 批量授权：

```
cscript slmgr.vbs -ipk [volume license key]
```

激活 KMS 授权：

```
cscript slmgr.vbs -ato
```

设置 KMS DNS SRV 记录：

```
cscript slmgr.vbs -skma [KMS FQDN]
```

确定计算机名称

```
ipconfig /all
Systeminfo.exe 或 Hostname.exe
```

重命名服务器核心计算机

已加入的域:

```
Netdom renamecomputer %computername% /NewName:new-name /UserD:domain-username /PasswordD:*
```

未加入的域:

```
Netdom renamecomputer %computername% /NewName:new-name
```

更改工作组:

```
Wmic computersystem where name="%computername%" call  joindomainorworkgroup name="[new workgroup name]"
```

安装角色或可选功能

```
Start /w Ocsetup [packagename]
```


注意：对于 Active Directory，应运行具有应答文件的 Dcpromo。

查看角色和可选功能包名称以及当前安装状态

```
oclist
```

启动任务管理器热键

```
ctrl-shift-esc
```

注销终端服务会话

```
Logoff
```

设置页面文件大小

禁用系统页面文件管理：

```
wmic computersystem where name="%computername%" set AutomaticManagedPagefile=False
```

配置页面文件：

```
wmic pagefileset where name="C:\\pagefile.sys" set InitialSize=500,MaximumSize=1000
```

配置时区、日期或时间

```
control timedate.cpl
```

配置区域和语言选项

```
control intl.cpl
```

手动安装管理工具或代理

```
Msiexec.exe /i [msipackage]
```

列出已安装的 MSI 应用程序

```
Wmic product
```

卸载 MSI 应用程序

```
Wmic product get 名称/value
```

显示安装的 MSI 应用程序：

```
wmic
product
```

Wmic 是一个很有用的操纵和管理 WMI 对象的命令，借助此命令通过 WMI 可以对 Server Core 进行绝大多数的管理操作(硬件管理、软件管理、网络管理等)。如要卸载安装的某一个 MSI 应用程序，则可以调用 Product 这个 WMI 对象的 Uninstall 方法，使用命令：

```
WMIC product where name="<name>" call uninstall
```

列出安装的驱动程序

```
Sc query type= driver
```

安装未包括的驱动程序

将驱动程序文件复制到服务器核心：

```
Pnputil -i -a [path]\[driver].inf
```

重命名网络适配器

```
netsh interface set interface name="Local Area Connection" newname="PrivateNetwork"
```

禁用网络适配器

```
netsh interface set interface name="Local Area Connection 2" admin=DISABLED
```

确定文件的版本

```
wmic datafile where name="c:\\windows\\system32\\ntdll.dll" get version
```

已安装的修补程序列表

```
wmic qfe list
```

安装修补程序

```
Wusa.exe [patchame].msu /quiet
```

配置代理

```
Netsh winhttp set proxy [proxy_name]:[port]
```

添加、删除、查询注册表值

```
reg.exe add /?
reg.exe delete /?
reg.exe query /?
```

其他开关

另外该脚本还有其他开关，用于进行一些特殊的配置。例如开启远程桌面、自动更新等。

```
systeminfo
```

此命令将显示计算机的详细信息。

3.11.1 任务 1：更改 Server Core 计算机名称

① 以管理员身份登录 Windows Server 核心服务器。
② 如图 3-109 所示，运行 HOSTNAME，显示当前计算机名称。
③ 运行 netdom renamecomputer WIN-M95F5DFAZC0/newname:FileServer，其中 WIN-M95F5DFAZC0 是现在的计算机名称，FileServer 是新的计算机名称。
④ 运行 shutdown /r /t 0，重启系统。

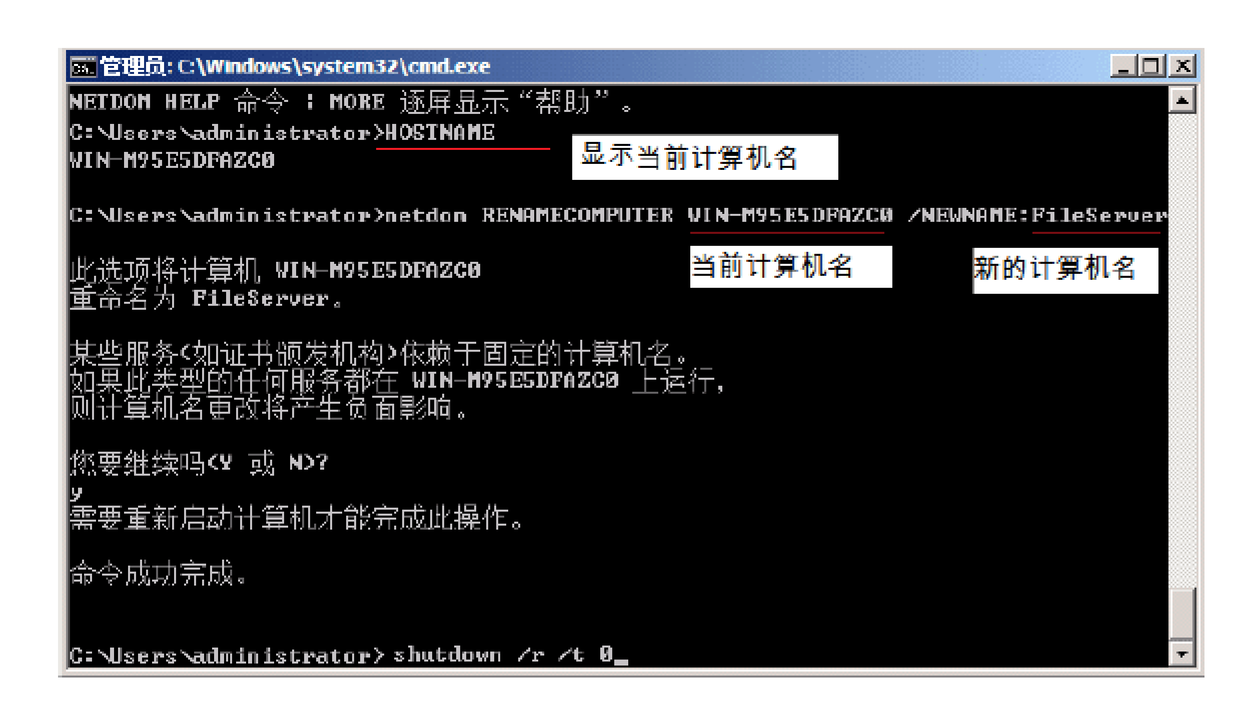


图 3-109　查看和更改计算机名

3.11.2　任务 2：配置 Windows 防火墙

启用 Windows 防火墙，如图 3-110 所示。

① 在命令行输入 netsh firewall set opmode enable，启用 Windows 防火墙。

② 默认情况下 Windows 防火墙已开启。

③ 在命令行输入 netsh firewall set opmode disable，关闭防火墙。

④ 在命令行输入 netsh firewall show state，查看防火墙状态。

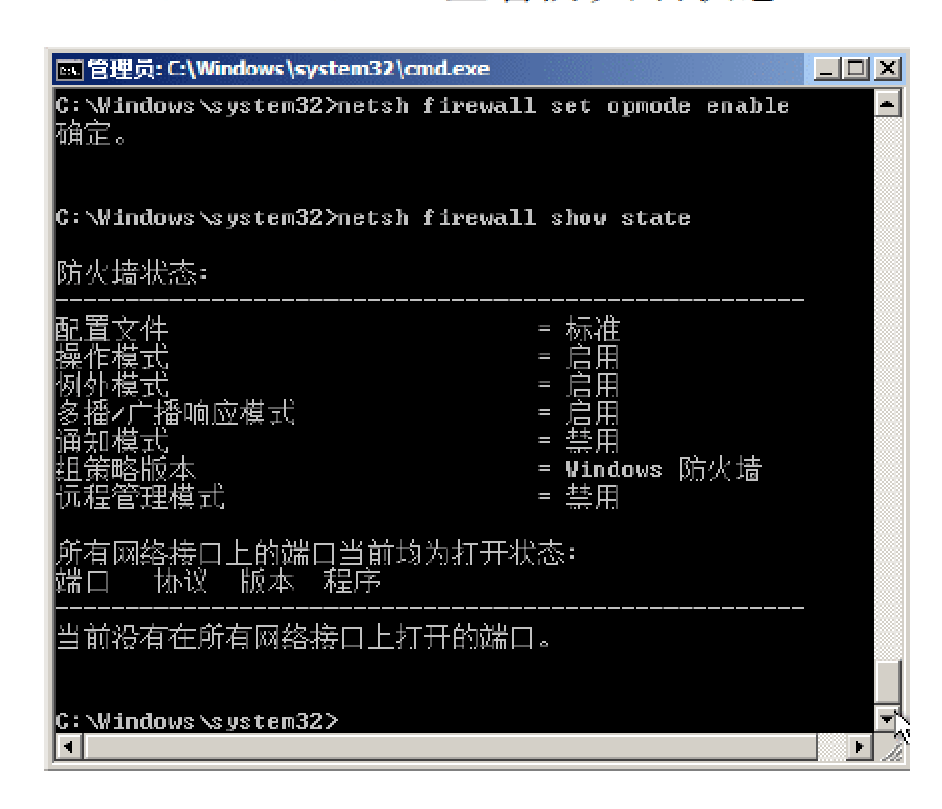


图 3-110　启用防火墙和禁用防火墙

⑤ 在命令行输入 netsh firewall add portopening UDP 53 DNS-Server，使该服务器计算机能响应客户端的 DNS 查询请求。



提示：*后续实战中将配置该服务器作为 DNS 服务器。*

⑥ 在命令行输入下列命令，使得其他计算机可以访问该计算机的“文件和打印服务”(该服务器为文件服务器)。

```
netsh firewall add portopening UDP 137 Netbios-ns
netsh firewall add portopening UDP 138 Netbios-dgm
netsh firewall add portopening TCP 139 Netbios-ssn
netsh firewall add portopening TCP 445 Netbios-ds
```

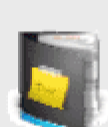
⑦ 在命令行输入 netsh firewall show config，查看防火墙配置。

从结果中可以看到“文件和打印共享”已经启用。

3.11.3 任务 3：为 Server Core 启用远程桌面

启用远程桌面。

① 在命令行输入 cscript SCregEdit.wsf /Ar 0。



提示：确定当前所在目录为 C:\Windows\System32。

② 在命令行输入 netsh firewall add portoepning TCP 3389 Remote-Desktop，打开远程桌面使用的端口。

3.11.4 任务 4：为 Windows Server Core 安装 DNS 角色

① 在命令行输入 oclist，查看角色和功能的安装信息。



提示：可以发现在默认情况下未安装任何角色和功能，所以称 Server Core 为最小化安装。

注意：记下打算安装的角色或者功能的名字，安装角色或功能时对大小写是敏感的，切记！切记！

② 如图 3-111 所示，输入 Start/w ocsetup DNS-Server-Core-Role，安装 DNS 服务器角色。

③ oclist | find “已安装”。

```
管理员: C:\Windows\system32\cmd.exe
C:\>copy td.txt \\10.7.10.44\c$
已复制         1 个文件。

C:\>Start /w  ocsetup DNS-Server-Core-Role

C:\>oclist | find "已安装"
    已安装:DNS-Server-Core-Role

C:\>_
```

图 3-111 安装 DNS 角色和查看安装好的角色

此命令用于显示 DNS 服务器是否安装成功。

第 4 章　管理本地用户和组

本章内容围绕如何在服务器上创建和管理本地用户和组。

可以使用 Windows Server 图形界面的管理工具管理 Windows Server Core 上的用户和组，管理访问其他服务器的凭据，管理存储的账户，使用用户账户控制保护系统安全。

关键词

- 本地用户账户
- 创建和管理用户
- 利用组来简化授权
- 管理存储的账号
- 管理 Windows core 上的用户和组
- 使用图形界面远程管理核心服务器
- 普通用户以管理员的身份打开管理工具

4.1 管理本地用户账户

Windows Server 2008 操作系统要求所有用户都要进行登录才能访问本地网络资源。Windows 通过实施交互式登录过程(提供用户身份验证)来保护资源。

用户账户是对计算机用户身份的标识，本地用户账户的账户、口令存在本地计算机中，只对本机有效，存储在本地安全账户数据库 SAM 中。

通过本地用户和组，可以为用户和组分配权利和权限，从而限制用户和组执行某些操作的能力。权利可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机。权限是与对象(通常是文件、文件夹或打印机)相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。

账户有以下三种不同类型。

- 标准。
- 管理员。
- 来宾。

每种账户类型为用户提供不同的计算机控制级别。标准账户是日常计算机使用中所使用的账户。管理员账户对计算机拥有最高的控制权限，并且应该仅在必要时才使用此账户。来宾账户主要供需要临时访问计算机的用户使用。

1. 标准用户账户

标准用户账户允许用户使用计算机的大多数功能，但是如果要进行的更改会影响计算机的其他用户或安全，则需要管理员的许可。

使用标准账户时，可以使用计算机上安装的大多数程序，但是无法安装或卸载软件和硬件，也无法删除计算机运行所必需的文件或者更改计算机上会影响其他用户的设置。如果使用的是标准账户，则某些程序可能要求用户提供管理员密码后才能执行某些任务。

2. 管理员账户

管理员账户就是允许你进行将影响其他用户的更改的用户账户。管理员可以更改安全设置，安装软件和硬件，访问计算机上的所有文件。管理员还可以对其他用户账户进行更改。

设置 Windows 时，将要求创建用户账户。此账户就是允许用户设置计算机以及安装用户想使用的所有程序的管理员账户。完成计算机设置后，会建议用户使用标准用户账户进行日常的计算机使用。使用标准用户账户比使用管理员账户更安全。

3. 来宾账户

来宾账户是供在计算机或域中没有永久账户的用户使用的账户。它允许人们使用计算机，但没有访问个人文件的权限。使用来宾账户的人无法安装软件或硬件，更改设置或者创建密码。必须打开来宾账户后才可以使用它。

4.1.1 内置的用户账户

本地用户和组 Microsoft 管理控制台 (MMC) 管理单元中的用户文件夹显示默认的用户账户以及创建的用户账户。这些默认的用户账户是在安装操作系统时自动创建的。下表描述了显示在本地用户和组中的每个默认用户账户。

打开“服务器管理器”窗口，单击“配置”→“本地用户和组”→“用户”选项，如图 4-1 所示，可以看到默认的用户账户。

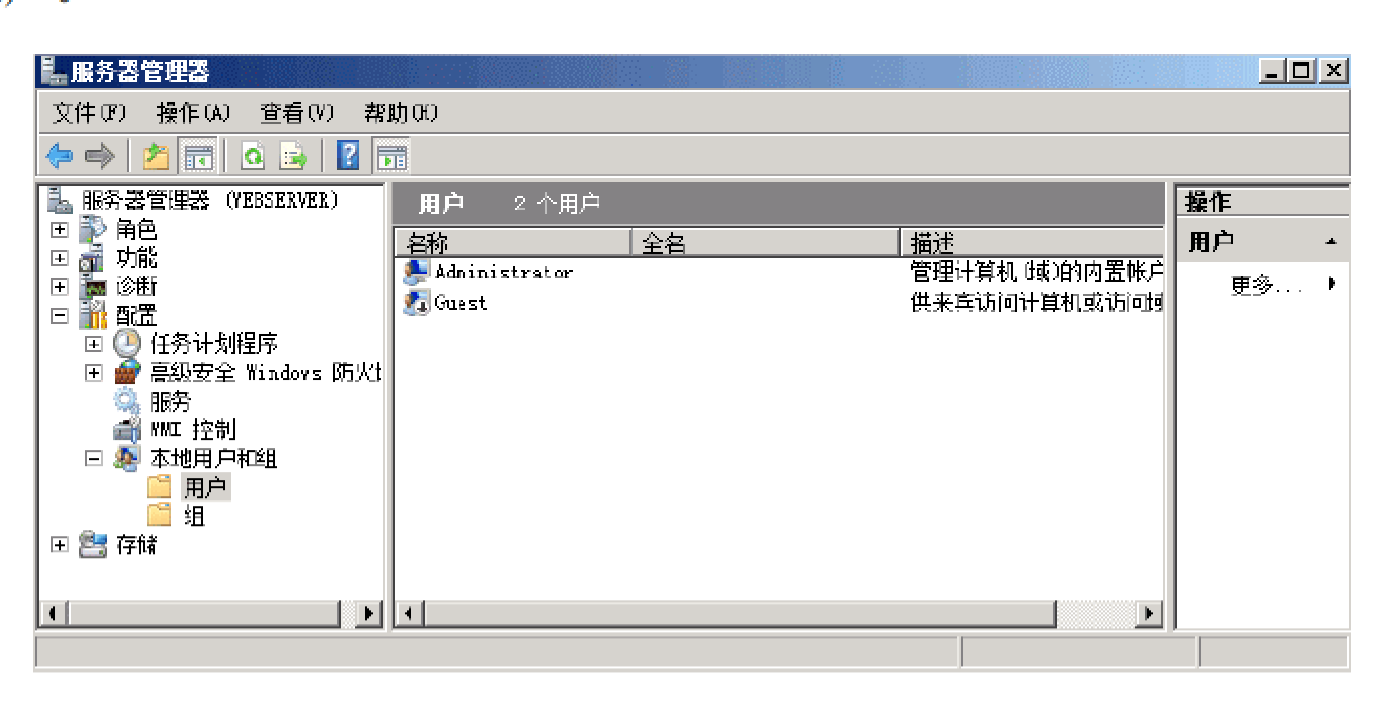


图 4-1 内置的用户账户

默认情况下，Administrator 账户处于禁用状态，但可以启用它。当它处于启用状态时，Administrator 账户具有对计算机的完全控制权限，并可以根据需要向用户分配用户权利和访问控制权限。该账户必须仅用于需要管理凭据的任务。强烈建议将此账户设置为使用强密码。Administrator 账户是计算机上 Administrators 组的成员。永远不可以从 Administrators 组删除 Administrator 账户，但可以重命名或禁用该账户。由于大家都知道 Administrator 账户存在于许多版本的 Windows 上，所以重命名或禁用此账户将使恶意用户尝试并访问该账户变得更为困难。


注意：即使已禁用了 Administrator 账户，仍然可以在安全模式下使用该账户访问计算机。

Guest 账户供在这台计算机上没有实际账户的人使用。如果某个用户的账户已被禁用，但还未删除，那该用户也可以使用 Guest 账户。Guest 账户不需要密码。默认情况下，Guest 账户是禁用的，但可以启用它。可以像任何用户账户一样设置 Guest 账户的权利和权限。默认情况下，Guest 账户是默认的 Guest 组的成员，该组允许用户登录计算机。其他权利及任何权限都必须由 Administrators 组的成员授予 Guests 组。默认情况下将禁用 Guest 账户，并且建议将其保持禁用状态。

4.1.2 创建本地用户

如图 4-2 所示，右击“用户”选项，在弹出的快捷菜单中选择“新用户”命令，在打开的对话框中输入用户名、全名、描述和密码。单击“创建”按钮。

若密码不符合密码策略要求将出现如图 4-3 所示的提示对话框。

> **提示：**Windows Server 2008 的安全策略默认要求用户的密码必须符合复杂性要求，因此输入的密码如果全是字符或全是数字会出现提示对话框。必须输入类似于“a1!”或“p@ssw0rd”这样的密码才能满足默认的安全密码。

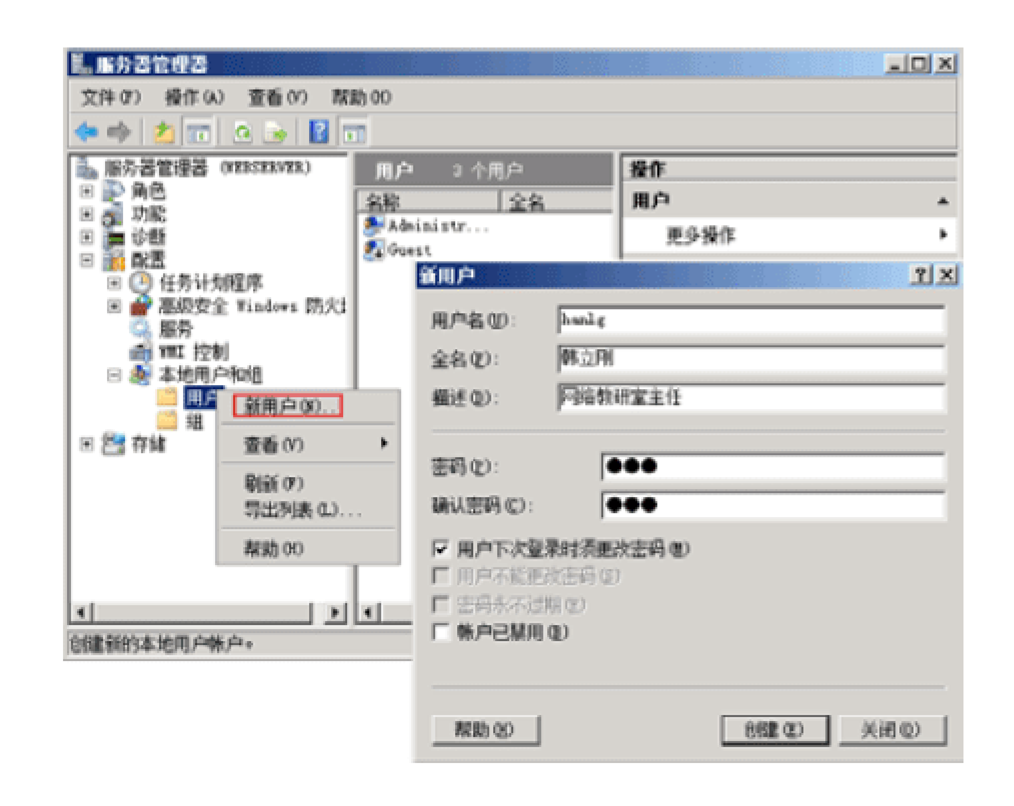


图 4-2　创建新用户

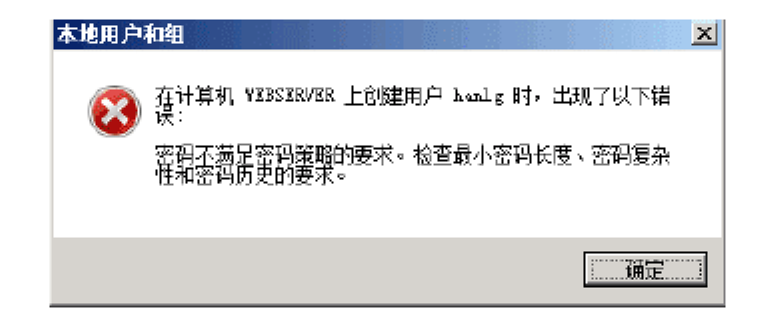


图 4-3　密码不符合策略要求

注意事项

- 若要执行此过程，必须提供本地计算机上 Administrator 账户的凭据(如果提示)，或必须是本地计算机上 Administrators 组的成员。
- 用户名不能与被管理的计算机上任何其他用户名或组名相同。用户名最多可以包含除下列字符外的 20 个大写字符或小写字符。
  - "、/、\、[、]、:、;、|、=、,、+、*、?、<、>、@。
  - 用户名不能只由句点(.)和空格组成。
- 在“密码”和“确认密码”文本框中，可以输入包含不超过 127 个字符的密码。但是，如果网络中包含运行 Windows 95 或 Windows 98 的计算机，应考虑使用不超过 14 个字符的密码。如果密码超过 14 个字符，则可能无法从运行 Windows 95 或 Windows 98 的计算机登录到网络。使用强密码和合适的密码策略有利于保护计算机免受攻击。

4.1.3　重设用户密码

① 如图 4-4 所示，右击用户账户，在弹出的快捷菜单中选择“设置密码”命令。

② 出现如图 4-5 所示的提示对话框，建议不要重设密码，最好更改。

③ 单击“继续”按钮，如图 4-6 所示，输入新密码，单击“确定”按钮。

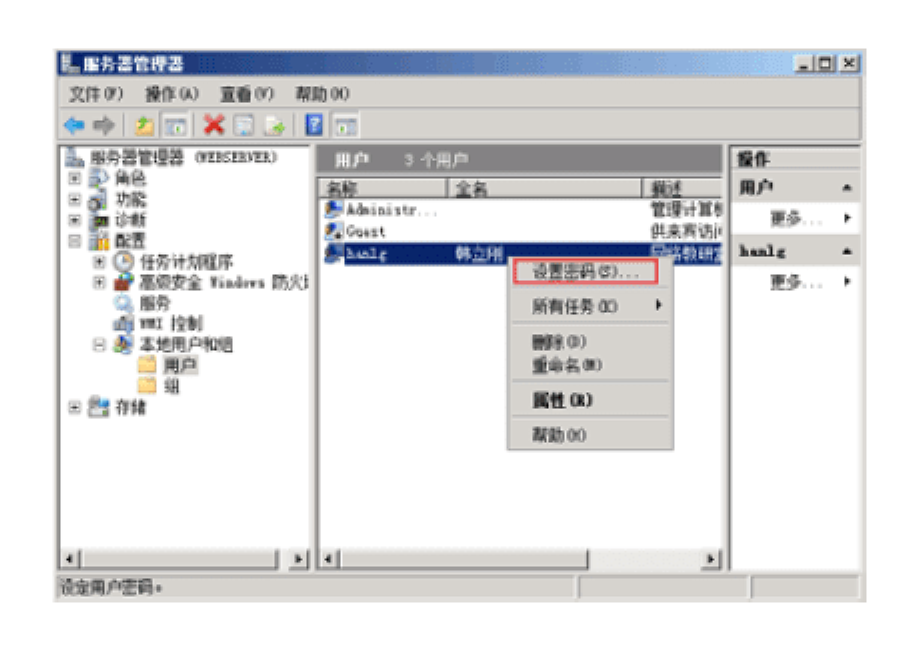


图 4-4　重设用户密码

若要执行此过程，必须提供本地计算机上 Administrator 账户的凭据(如果提示)，或必须是本地计算机上 Administrators 组的成员。

密码提供了防止对计算机进行未授权的访问的第一道防

线。密码越强，就越能保护计算机免受黑客和恶意软件的侵害。应确保计算机上所有账户使用的都是强密码。如果使用的是企业网络，网络管理员可能需要你使用强密码。

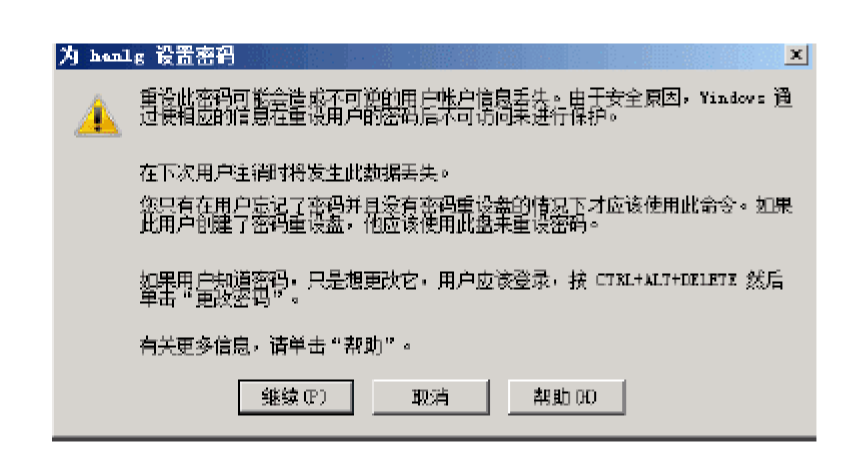


图 4-5　建议不要重设密码而要更改密码

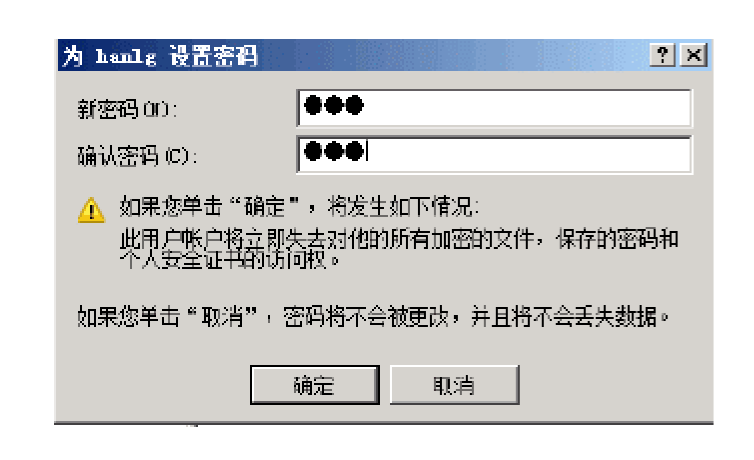


图 4-6　输入新密码

强密码(或弱密码)的构成如下。

- 长度至少为 8 个字符。
- 不包含用户名、真实姓名或公司名称。
- 不包含完整的单词。
- 与先前的密码截然不同。

包含下列 4 类字符的每一种。

- 大写字母。
- 小写字母。
- 数字。
- 键盘上的符号(键盘上所有未定义为字母和数字的字符)和空格。

强密码可以提高计算机和网络的安全性。为了保护信息的安全，一旦在本地用户账户上重设了用户密码，部分类型的信息将不能再使用，这些信息包括：

- 使用用户公钥加密的电子邮件。
- 计算机中保存的 Internet 密码。
- 用户已加密的文件。

若要避免丢失这种类型的数据，则不要重设用户的密码。当创建新的本地用户账户时，用户应创建一张密码重设盘。以后如果用户忘记了密码，可以使用密码重设盘来重设密码，防止数据损失。但是如果用户忘记了域用户账户的密码，则必须手工重设该密码。

4.1.4　创建密码重设盘

创建密码重设盘，不论密码更改过多少次，如果忘记了计算机密码，则可以使用密码重设盘创建一个新密码。建议在创建密码时创建密码重设盘，以便不会失去对文件和信息的访问权限。

① 将 U 盘插入计算机，下面的步骤将 U 盘设置成密码重设盘。

② 选择“开始”→“控制面板”命令，如果是传统的“开始”菜单，则选择“开始”→“设置”→“控制面板”命令，在打开的“控制面板”窗口中单击左面的“经典视图”选项，单击“用户帐户”图标，如图 4-7 所示。

③ 如图 4-8 所示，单击“创建密码重设盘”选项。

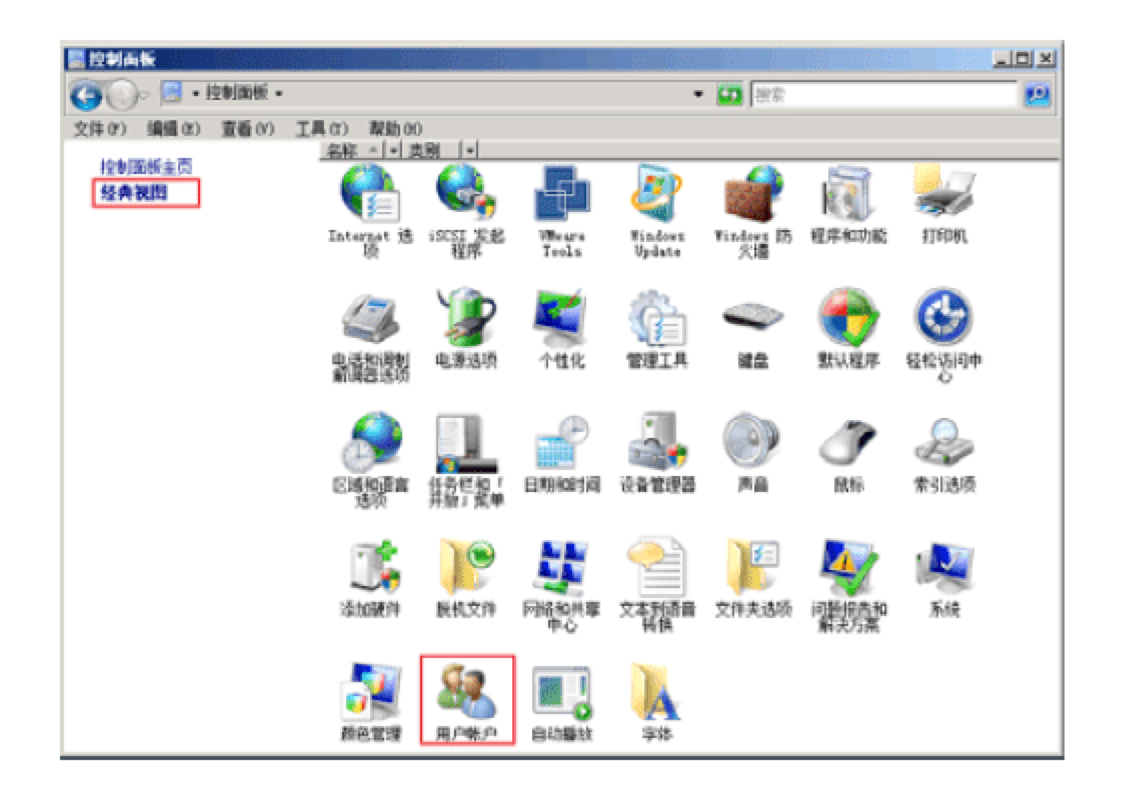


图 4-7　单击"用户帐户"图标



图 4-8　创建密码重设盘

④　如图 4-9 所示，在出现的向导对话框中，单击"下一步"按钮。

⑤　如图 4-10 所示，选择刚才插入的 U 盘，单击"下一步"按钮。

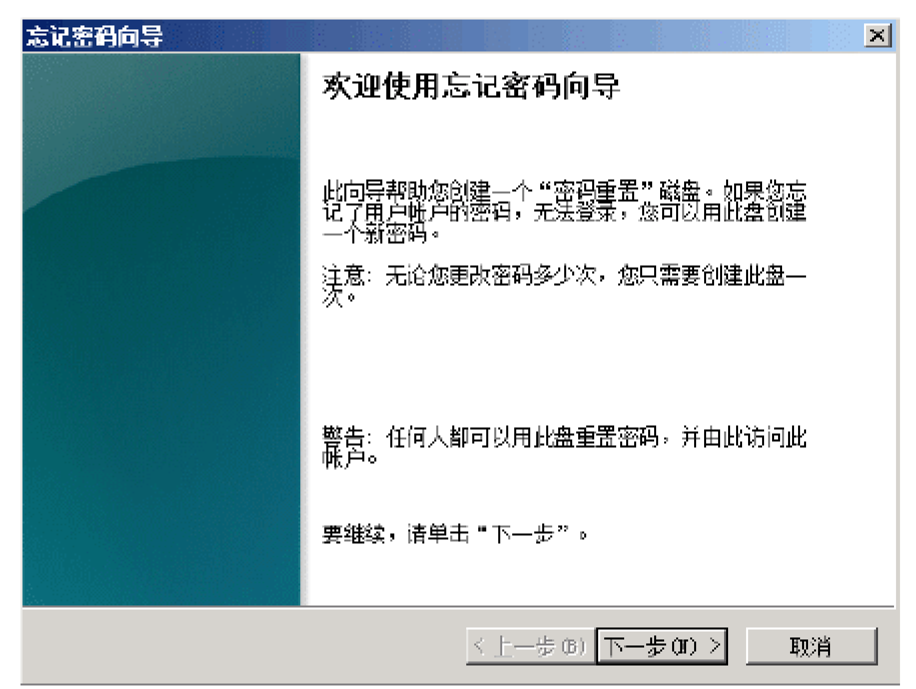


图 4-9　欢迎界面

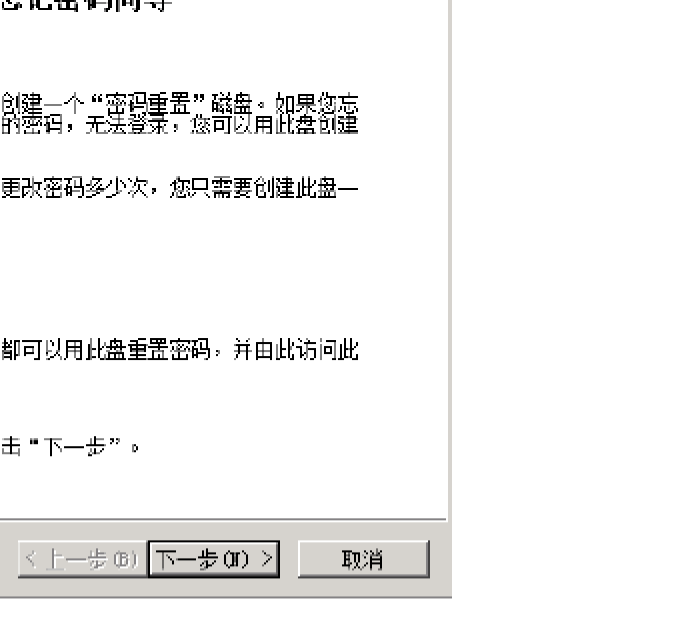


图 4-10　选择 U 盘

⑥　如图 4-11 所示，在出现的"当前用户帐户密码"界面中，输入当前用户密码，单击"下一步"按钮，完成。此时在 U 盘上创建了一个 userkey.psw 文件。

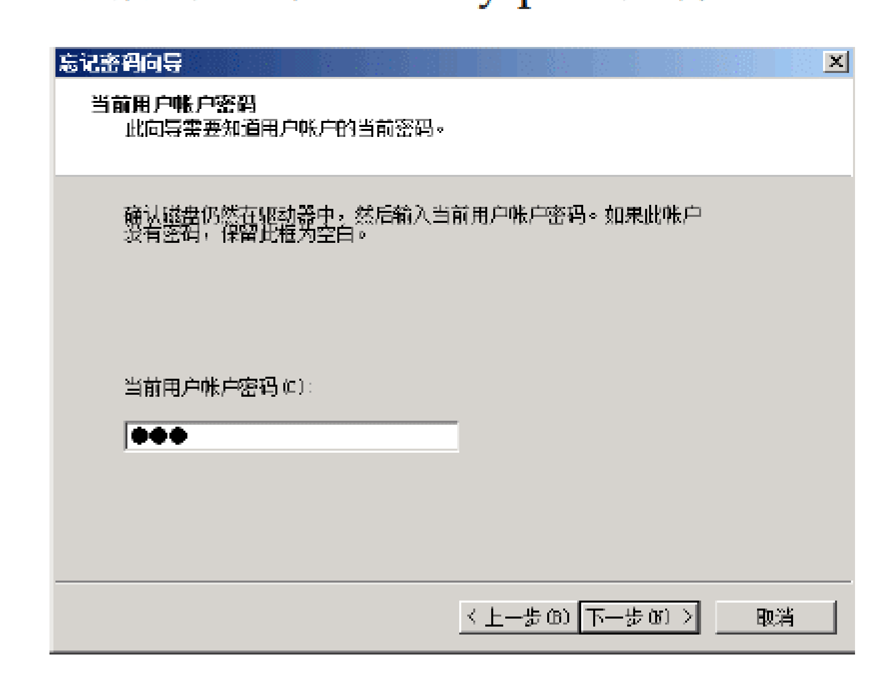


图 4-11　输入当前用户的密码

4.1.5　使用密码重设盘重设密码

如果是忘记密码，需要使用密码重设盘重新设置新密码。

① 输入错误登录密码后，会出现重设密码提示框，如图 4-12~图 4-14 所示。

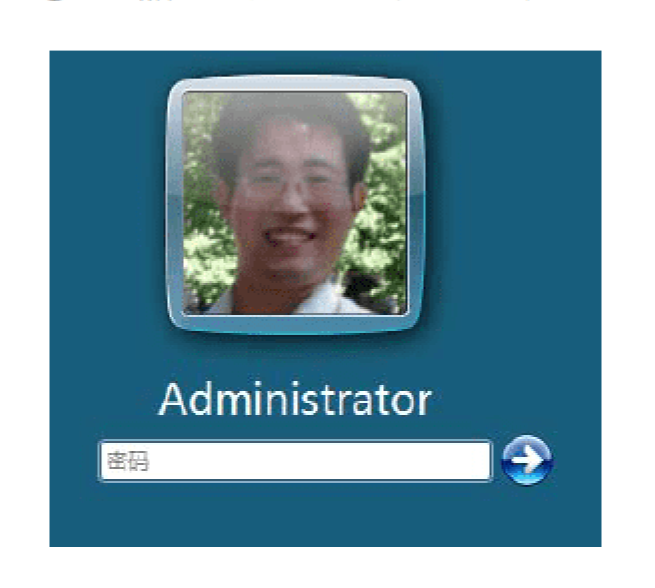


图 4-12　输入错误密码登录



图 4-13　提示密码不正确



图 4-14　出现重设密码

② 单击“重设密码”按钮，在出现的对话框中，单击“下一步”按钮，如图 4-15 所示。

③ 如图 4-16 所示，选中 U 盘，单击“下一步”按钮。

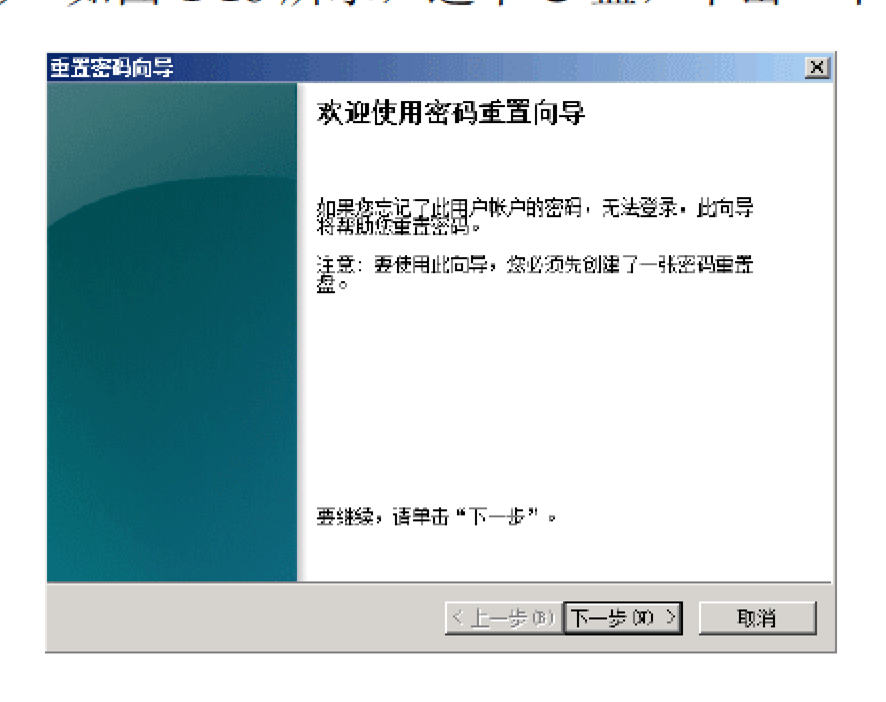


图 4-15　密码重设向导

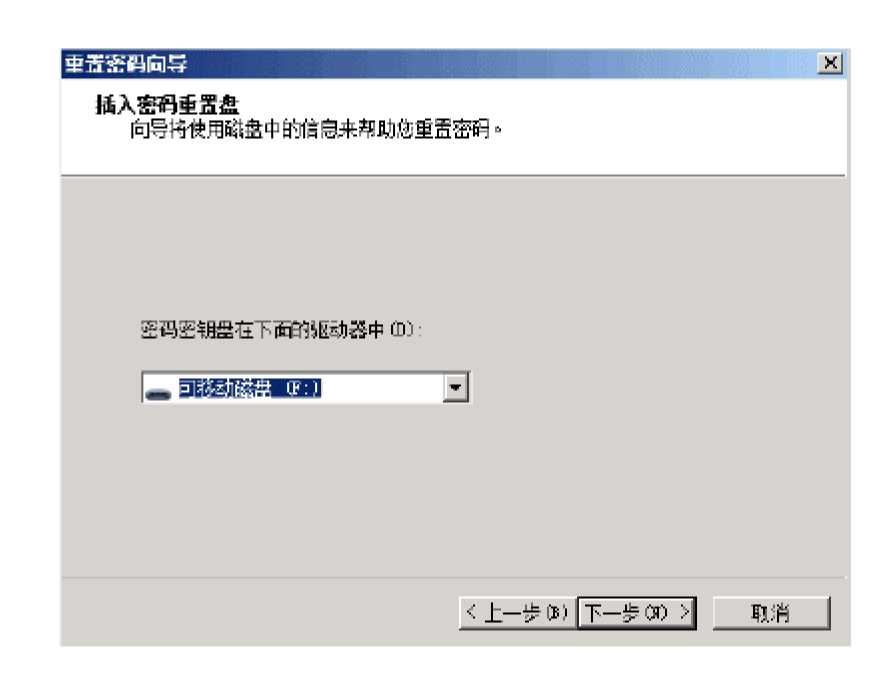


图 4-16　选择 U 盘

④ 如图 4-17 所示，输入新密码和密码提示，单击“下一步”按钮。

⑤ 如图 4-18 所示，单击“完成”按钮，完成密码重设。

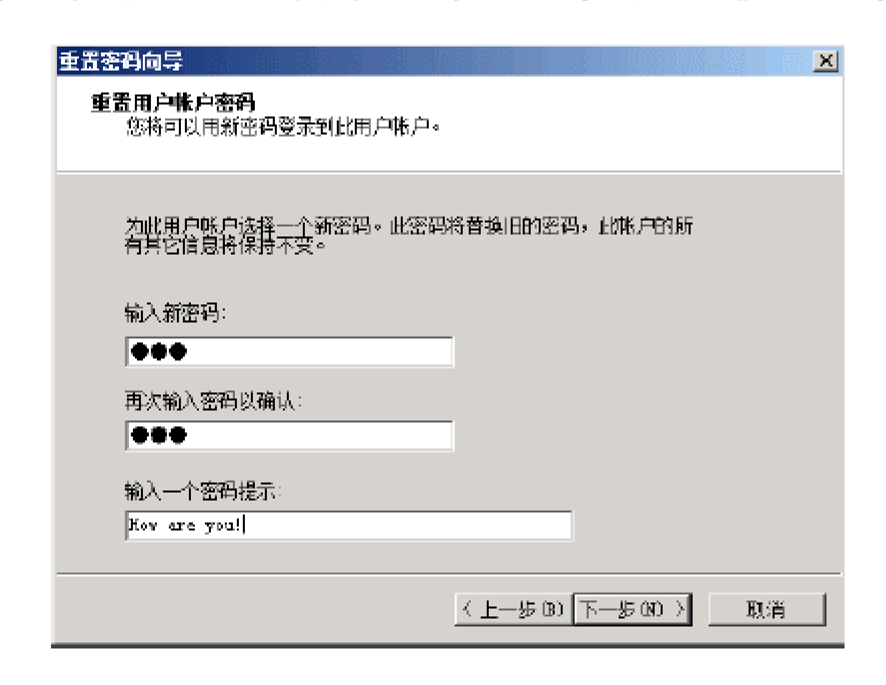


图 4-17　输入新密码

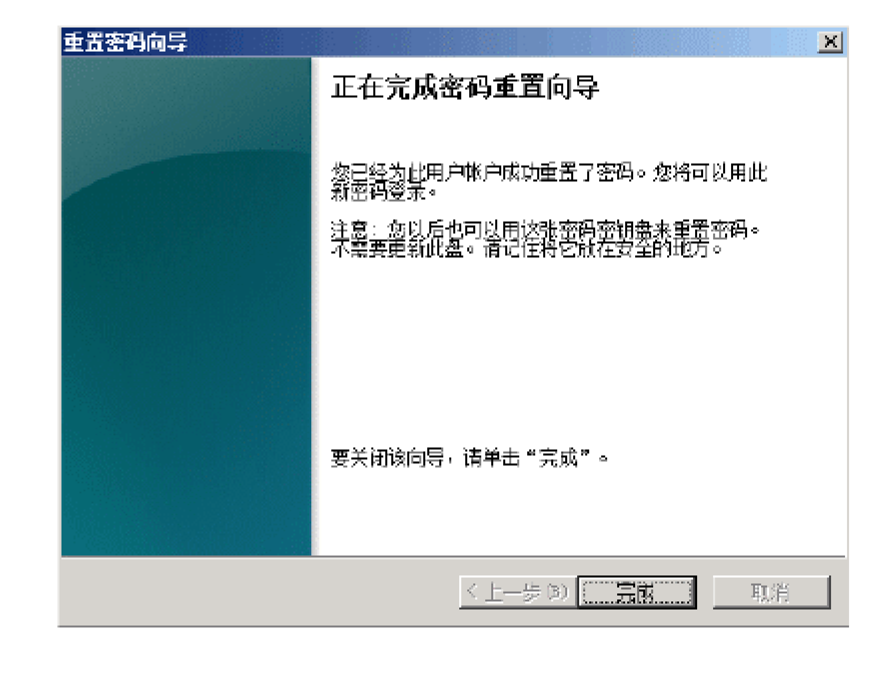


图 4-18　完成密码重设

4.1.6　管理存储的账号

如果你经常访问某个服务器的共享文件夹，每次都需要输入访问服务器的账户和密码，则可以将访问该服务器的凭据保存起来。下面是访问文件服务器 10.7.1.4 上的共享文件夹，如图 4-19 所示，需要输入该文件服务器上的账户和密码，如图 4-20 所示。

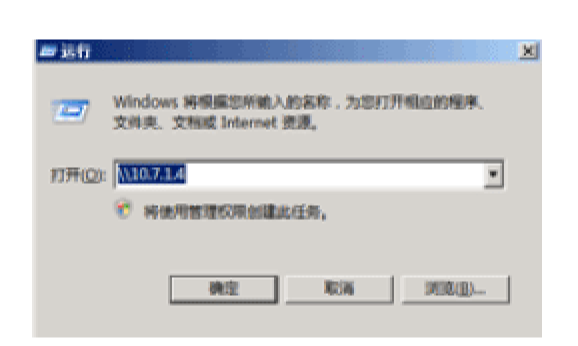



图 4-19　访问服务器上的共享资源

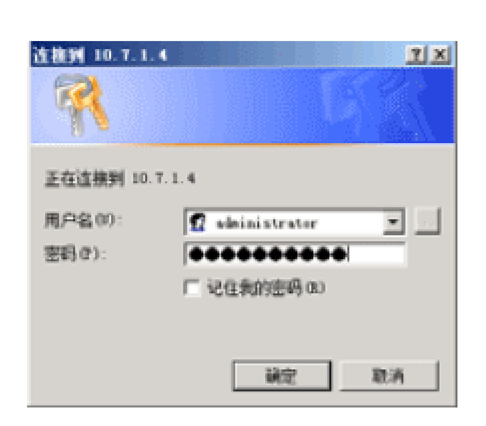


图 4-20　输入服务上的账户和密码

下面的操作会保存访问该服务器的网络凭据。

① 选择“开始”→“控制面板”命令，如果是传统的“开始”菜单，选择“开始”→“设置”→“控制面板”命令，在打开的“控制面板”窗口中单击左面的“经典视图”选项，单击“用户帐户”图标打开如图 4-21 所示的对话框。



图 4-21　管理网络密码

② 如图 4-22 所示，在出现的“存储的用户名和密码”对话框中，单击“添加”按钮。

③ 如图 4-23 所示，输入服务器的地址、访问该服务器用到的用户名和密码，单击“确定”按钮。



图 4-22　存储的用户名和密码

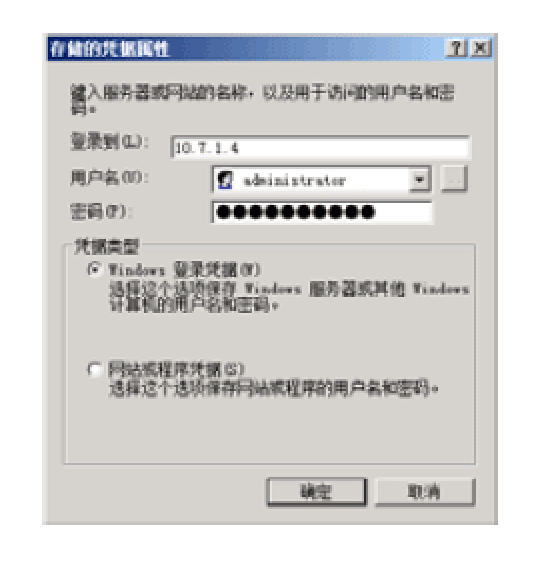


图 4-23　添加访问服务器的用户名和密码

④ 再次访问该服务时发现不再需要输入账户和密码。

如果想用计算机名访问 10.7.1.4 上的共享资源，如图 4-24 所示，则需要再添加一个登录到服务器名的网络凭据，如图 4-25 所示。

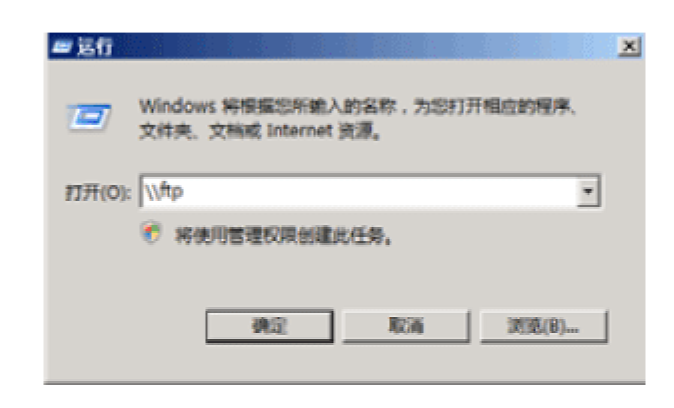


图 4-24　使用计算机名访问



图 4-25　添加使用计算机名访问的凭据

4.1.7　禁用或激活本地用户

① 打开“服务器管理器”窗口。

② 如图 4-26 所示，在控制台树中，单击“用户”选项，右击要更改的用户账户，在弹出的快捷菜单中选择“属性”命令。

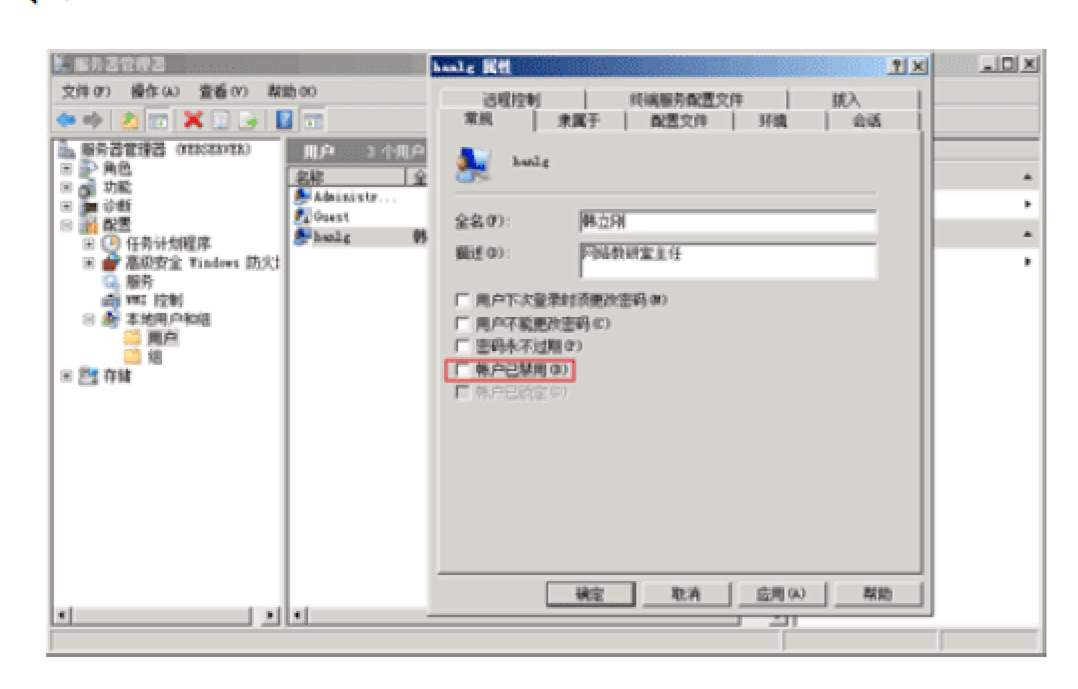


图 4-26　禁用用户

执行以下任一操作。

- 若要禁用所选的用户账户，应选中“帐户已禁用”复选框。
- 若要激活所选的用户账户，应取消选中“帐户已禁用”复选框。

注意事项

- 若要执行此过程，必须提供本地计算机上 Administrator 账户的凭据(如果提示)，或必须是本地计算机上 Administrators 组的成员。
- 禁用某个用户账户时，将不允许该用户登录。该账户将出现在详细信息窗格中，图标上显示一个号。
- 在激活已禁用的账户之前，应确保该账户不是因安全原因而被锁定的。
- 用户账户被激活后，该用户就可以正常登录。

4.1.8　删除本地用户账户

① 打开“服务器管理器”窗口。

② 在控制台树中，单击“用户”选项。

③ 右击要删除的用户账户，在弹出的快捷菜单中选择“删除”命令。

注意事项

- 若要执行此过程，必须提供本地计算机上 Administrator 账户的凭据(如果提示)，或必须是本地计算机上 Administrators 组的成员。
- 当需要删除一个用户账户时，建议首先禁用该账户。确信禁用账户不会引起问题时，便可放心地删除该账户。
- 不能恢复已删除的用户账户。

■ 不能删除 Administrator 账户和 Guest 账户。

4.1.9 重命名本地用户账户

① 打开“服务器管理器”窗口。

② 在控制台树中，单击“用户”选项。如图 4-27 所示，右击要重命名的用户账户，在弹出的快捷菜单中选择“重命名”命令。

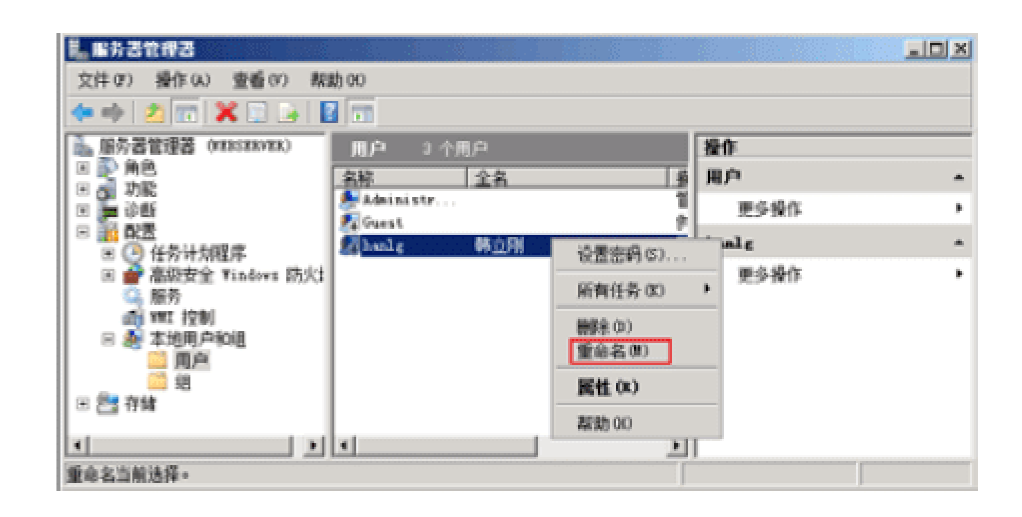


图 4-27 重命名用户权限不变

③ 输入新的用户名，然后按 Enter 键。

注意事项

■ 若要执行此过程，必须提供本地计算机上 Administrator 账户的凭据(如果提示)，或必须是本地计算机上 Administrators 组的成员。

■ 由于重命名的用户账户会保留其安全标识符 (SID)，因此也保留其他所有属性，如描述、密码、组成员身份、用户配置文件、账户信息以及任何已指派的权限和用户权利。

■ 用户名不能与被管理的计算机上任何其他用户名或组名相同。用户名最多可以包含除下列字符外的 20 个大写字符或小写字符："、/、\、[、]、:、;、|、=、,、+、*、?、<、>、@。

如图 4-28 所示，查看当前用户的 SID，在命令行下输入 whoami /user，显示当前用户的 SID。管理员的 SID 默认后三位是 500。

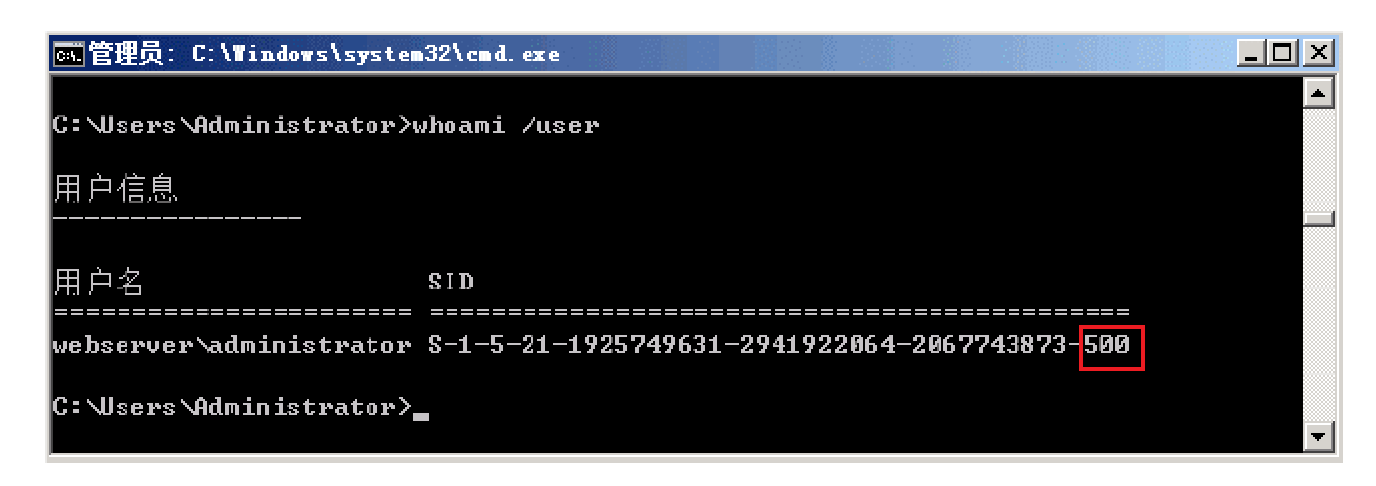


图 4-28 查看用户的 SID

4.2 管理本地组

组是用户账户的集合，利用组可以管理对共享资源的访问。这样的共享资源包括网络文件夹、文件、目录和打印机。利用组，可以将访问共享资源的权限一次授予某个组，而不是单独授予多个用户。利用组可以简化授权。

如销售部的成员可以访问产品的成本信息，不能访问公司员工的工资信息，而人事部的员工可以访问员工的工资信息却不能访问产品成本信息。当一个销售部的员工调到人事部后，如果我们的权限控制是以每个用户为单位进行控制，则权限设置相当麻烦而且容易出错；如果我们用组进行管理则相当简单，我们只需将该用户从销售组中删除再将之添加进人事组即可。如果销售部门的员工兼职人事部门工作，需要将其加入到人事组，则该用户就有了两个组的权限。

4.2.1　默认本地组

下面列出了每个组的默认用户权利。这些用户权利是在本地安全策略中分配的。

- Administrators：此组的成员具有对计算机的完全控制权限，并且他们可以根据需要向用户分配用户权利和访问控制权限。Administrator 账户是此组的默认成员。当计算机加入域中时，Domain Admins 组会自动添加到此组中。因为此组可以完全控制计算机，所以向其中添加用户时要特别谨慎。以下列出了该组默认用户权利。
  - 从网络访问此计算机。
  - 调整进程的内存配额。
  - 允许本地登录。
  - 允许通过终端服务登录。
  - 备份文件和目录。
  - 跳过遍历检查。
  - 更改系统时间。
  - 更改时区。
  - 创建页面文件。
  - 创建全局对象。
  - 创建符号链接。
  - 调试程序。
  - 从远程系统强制关机。
  - 身份验证后模拟客户端。
  - 提高日程安排的优先级。
  - 装载和卸载设备驱动程序。
  - 作为批处理作业登录。
  - 管理审核和安全日志。
  - 修改固件环境变量。
  - 执行卷维护任务。
  - 配置单一进程。
  - 配置系统性能。
  - 从扩展坞中取出计算机。
  - 还原文件和目录。
  - 关闭系统。
  - 获得文件或其他对象的所有权。
- Backup Operators：此组的成员可以备份和还原计算机上的文件，而不管保护这些文件的权限如

何。这是因为执行备份任务的权利要高于所有文件权限。此组的成员无法更改安全设置。

- 从网络访问此计算机。
- 允许本地登录。
- 备份文件和目录。
- 跳过遍历检查。
- 作为批处理作业登录。
- 还原文件和目录。
- 关闭系统。

■ Cryptographic Operators：已授权此组的成员执行加密操作。没有默认的用户权利。

■ Distributed COM Users：允许此组的成员在计算机上启动、激活和使用 DCOM 对象。没有默认的用户权利。

■ Guests：该组的成员拥有一个在登录时创建的临时配置文件，在注销时，此配置文件将被删除。来宾账户(默认情况下已禁用)也是该组的默认成员。没有默认的用户权利。

■ IIS_IUSRS：这是 Internet 信息服务 (IIS) 使用的内置组。没有默认的用户权利。

■ Network Configuration Operators：该组的成员可以更改 TCP/IP 设置，并且可以更新和发布 TCP/IP 地址。该组中没有默认的成员。没有默认的用户权利。

■ Performance Log Users：该组的成员可以从本地计算机和远程客户端管理性能计数器、日志和警报，而不用成为 Administrators 组的成员。没有默认的用户权利。

■ Performance Monitor Users：该组的成员可以从本地计算机和远程客户端监视性能计数器，而不用成为 Administrators 组或 Performance Log Users 组的成员。没有默认的用户权利。

■ Power Users：默认情况下，该组的成员拥有不高于标准用户账户的用户权利或权限。在早期版本的 Windows 中，Power Users 组专门为用户提供特定的管理员权利和权限执行常见的系统任务。在此版本 Windows 中，标准用户账户具有执行最常见配置任务的权限，例如更改时区。对于需要与早期版本的 Windows 相同的 Power User 权利和权限的旧应用程序，管理员可以应用一个安全模板，此模板可以启用 Power Users 组，以假设具有与早期版本的 Windows 相同的权利和权限。没有默认的用户权利。

■ Remote Desktop Users：该组的成员可以远程登录计算机。允许通过终端服务登录。

■ Replicator：该组支持复制功能。Replicator 组的唯一成员应该是域用户账户，用于登录域控制器的复制器服务。不能将实际用户的用户账户添加到该组中。没有默认的用户权利。

■ Users：该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定计算机。该组的成员无法共享目录或创建本地打印机。默认情况下，Domain Users、Authenticated Users 以及 Interactive 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员。以下列出了该组默认用户权利。

- 从网络访问此计算机。
- 允许本地登录。
- 跳过遍历检查。
- 更改时区。
- 增加进程工作集。
- 从扩展坞中取出计算机。
- 关闭系统。

■ 提供远程协助帮助程序：该组的成员可以向此计算机用户提供远程协助。没有默认的用户权利。

4.2.2　创建本地组

如果默认本地组不能满足用户的授权要求，则需要创建新的组。

① 打开“服务器管理器”窗口，在控制台树中，右击“组”选项，在弹出的快捷菜单中选择“新建组”命令。

② 如图 4-29 所示，在“组名”文本框中，输入新组的名称，在“描述”文本框中，输入新组的描述，单击“添加”按钮。

③ 在“选择用户、计算机或组”对话框中，执行下列操作。

■ 若要向该组添加用户账户或组账户，则在“输入对象名称来选择”文本框中，输入要添加的用户账户或组账户的名称，然后单击“确定”按钮。

■ 若要向该组添加计算机账户，则单击“对象类型”文本框，选中“计算机”复选框，然后单击“确定”按钮。在“输入对象名称来选择”文本框，输入要添加的计算机账户的名称，然后单击“确定”按钮。

④ 在“新建组”对话框中单击“创建”按钮，然后单击“关闭”按钮。



图 4-29　创建组

4.2.3　管理组的成员

打开“服务器管理器”窗口，双击“组”选项，在组的属性对话框中，如图 4-30 所示，可以看到该组的成员，单击“添加”按钮，可以添加用户到该组。选中其中的成员，单击“删除”按钮，可以将用户从该组删除。

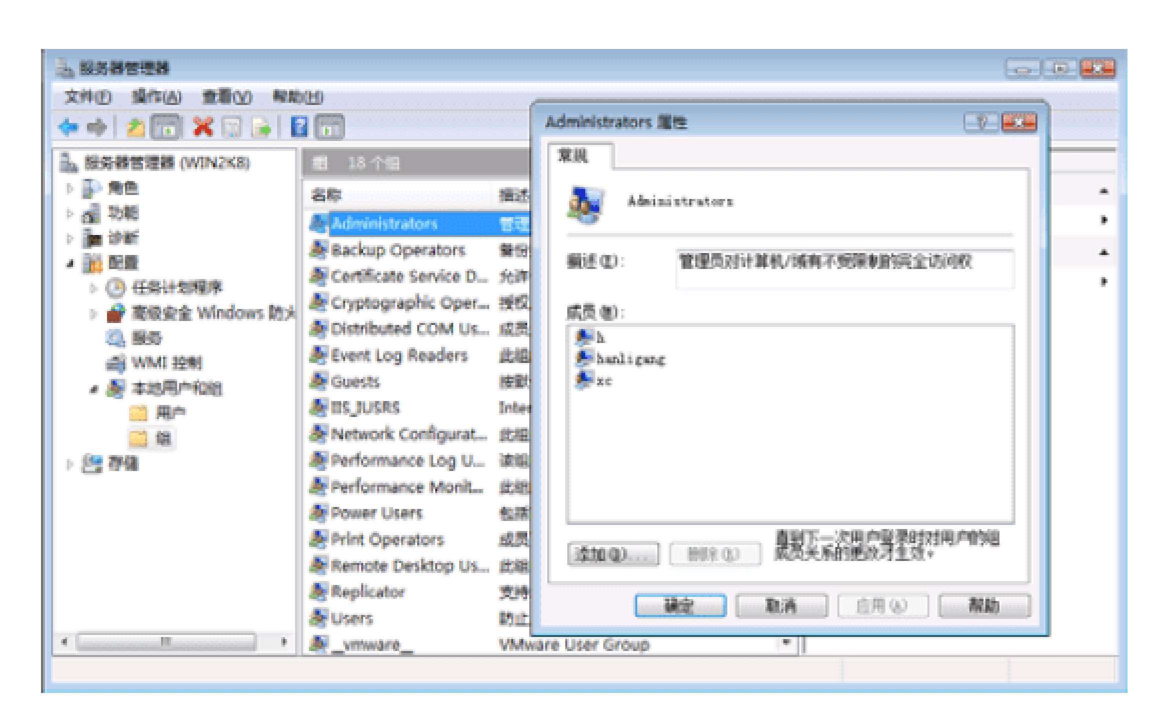


图 4-30　管理组的成员

4.2.4　管理用户所属的组

打开“服务器管理器”窗口，双击用户账户，打开用户属性对话框，如图 4-31 所示。切换到“隶属于”选项卡，可以看到用户所属的组。单击“添加”按钮，可以将该用户添加到某个组。选中某个用户，单击

“删除”按钮，可以将该用户从某个组删除。

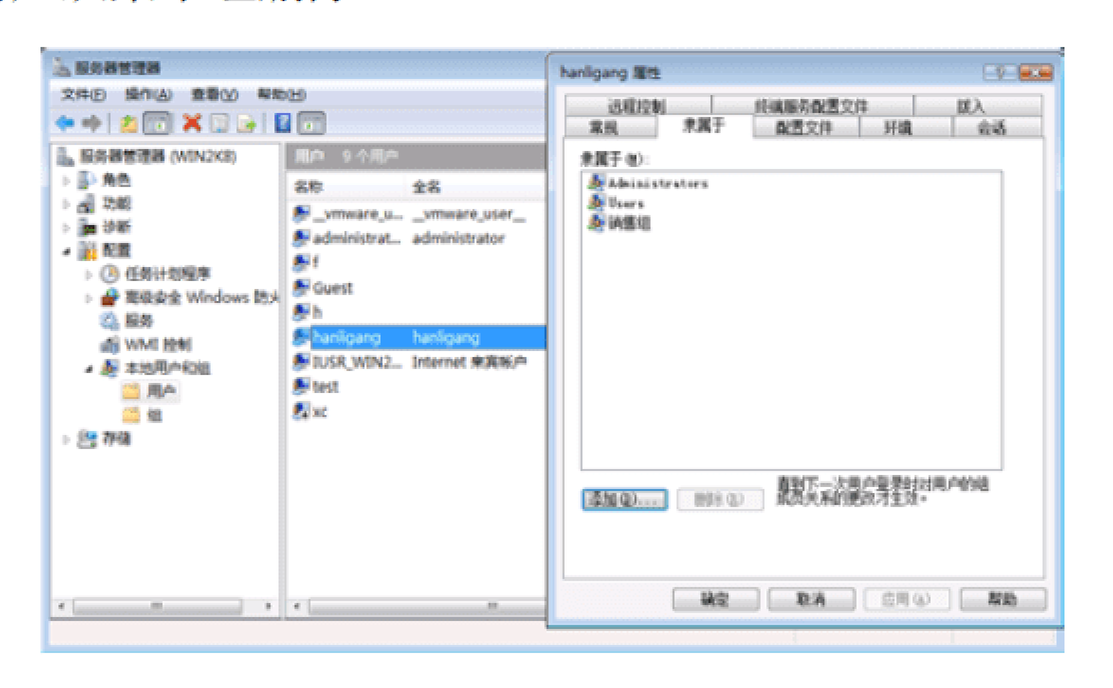


图 4-31　查看用户所属的组

4.2.5　删除本地组

① 打开“服务器管理器”窗口。

② 右击要删除的组，在弹出的快捷菜单中选择“删除”命令即可。

注意事项

- 无法删除系统默认组。
- 不能恢复已删除的组。
- 删除某个本地组将仅删除该组。而不会删除作为该组成员的用户账户、计算机账户或组账户。
- 如果删除某个组，然后用相同的组名创建另一个组，则必须为新组设置新的权限。新组将不会继承分配给旧组的权限。

4.3　管理 Server Core 上的账户和组

由于 Windows Server Core 操作系统只有命令行界面，因此用户账户和组的管理只能在命令行下实现。另外，可以在有图形界面的 Windows Server 2008 的服务器上使用图形化的管理工具管理 Server Core 上的账户。

4.3.1　在 Server Core 上使用命令行管理用户和组

以管理员的身份登录到服务器核心。

① 如图 4-32 所示，输入 net user，查看服务器上的所有账户。

② 输入 net user zhang a1! /add，添加一个 zhang 用户，密码是 a1!。

③ 输入 net user zhang a2!，更改用户的密码为 a2!。

④ 输入 net user zhang，查看用户详细信息。

⑤ 输入 net user zhang /del。

⑥ 输入 net localgroup managers /add，创建一个组 managers。

⑦ 输入 net logcalgroup managers zhang /add，将 zhang 用户添加到 managers 组，如图 4-33 所示。

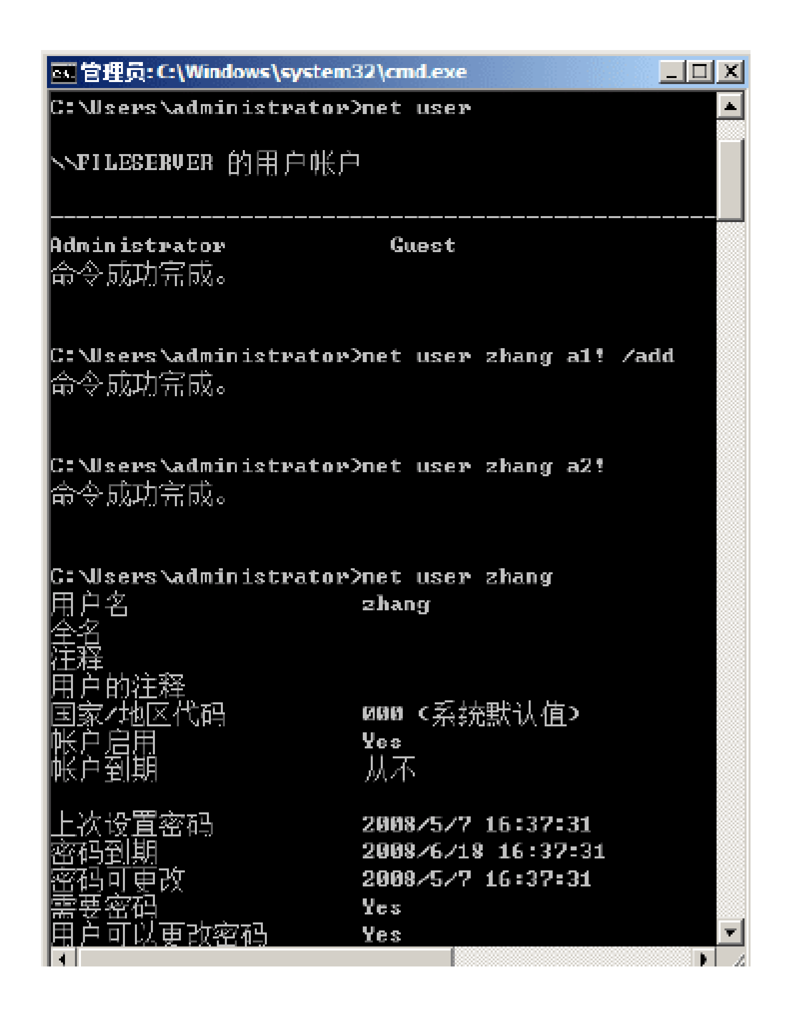


图 4-32　管理 Server Core 用户

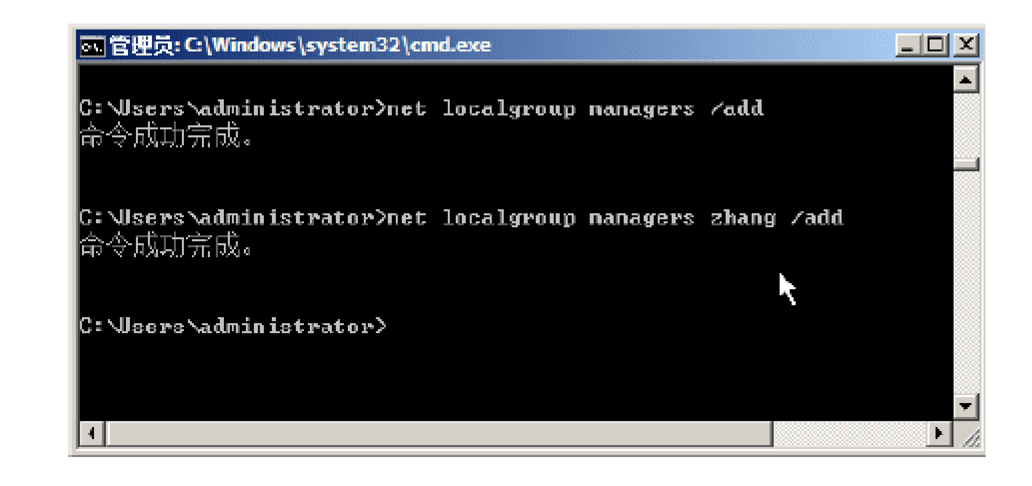


图 4-33　将用户添加到组

4.3.2　使用 Windows Server 图形界面管理 Windows Server Core

以下配置将会实现用安装了 Windows Server 2008 企业版的 WebServer 管理工具来管理 Windows Server Core。

① 以管理员的身份登录到 Windows Server Core。

② 输入 ipconfig，查看 IP 地址。

③ 输入 netsh firewall set opmode disable，关闭 Windows 防火墙。如图 4-34 所示，如果不关闭防火墙，可以运行以下命令只打开特定端口：

```
netsh firewall set opmode enable
netsh firewall add portopening TCP 445 Netbios-ds
```

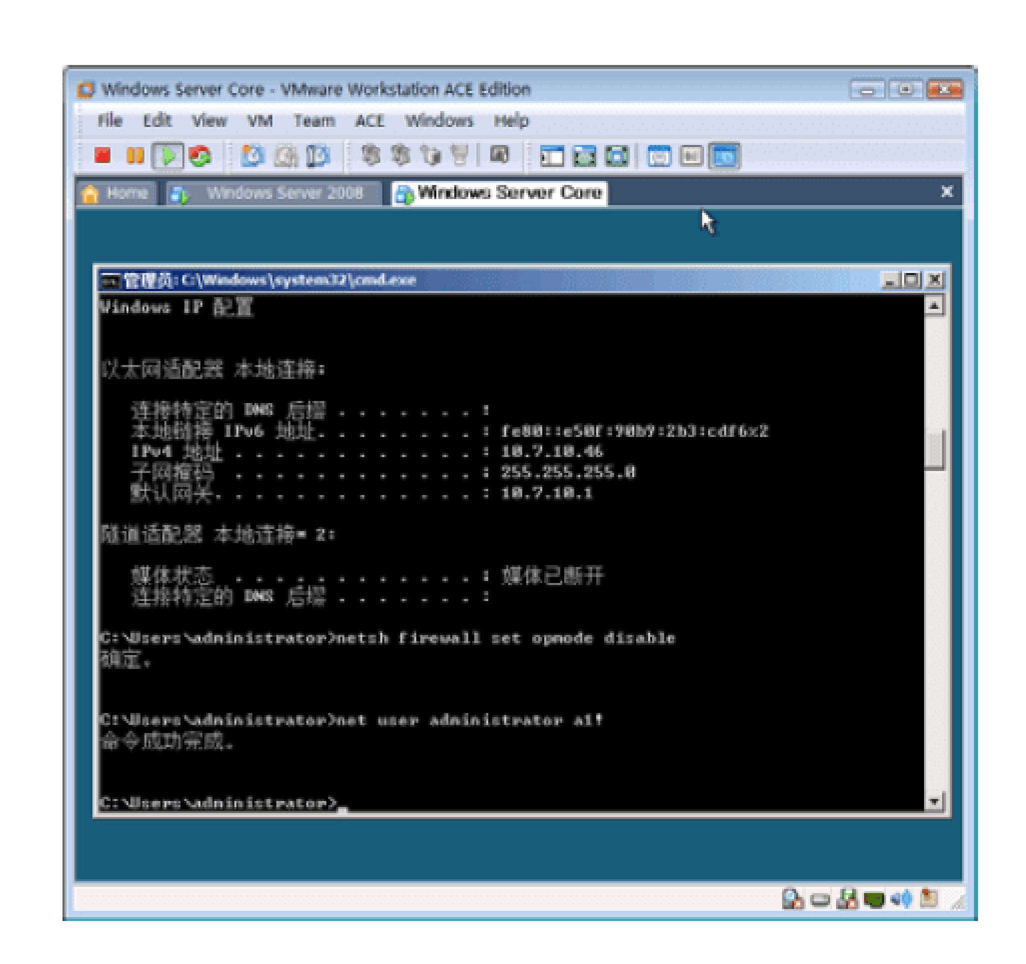


图 4-34　关闭防火墙

④ 输入 net user administrator a1!，更改管理员 Administrator 的密码与 WebServer 上计算机中管

理员 Administrator 账户的密码一样，这样，在 WebServer 使用图形界面管理工具连接 Windows Server Core 时才能成功。

⑤ 在安装 Windows Server 2008 企业版的 WebServer 上，以管理员 Administrator 密码 a1! 登录。

⑥ 如图 4-35 所示，选择“开始”→“运行”命令，打开“运行”对话框，输入 mmc，单击“确定”按钮。



提示：MMC 是微软管理控制台，可以将多个管理单元添加到一个管理控制台，使用起来较为方便。

⑦ 如图 4-36 所示，在控制台窗口，选择“文件”→“添加/删除管理单元”命令。

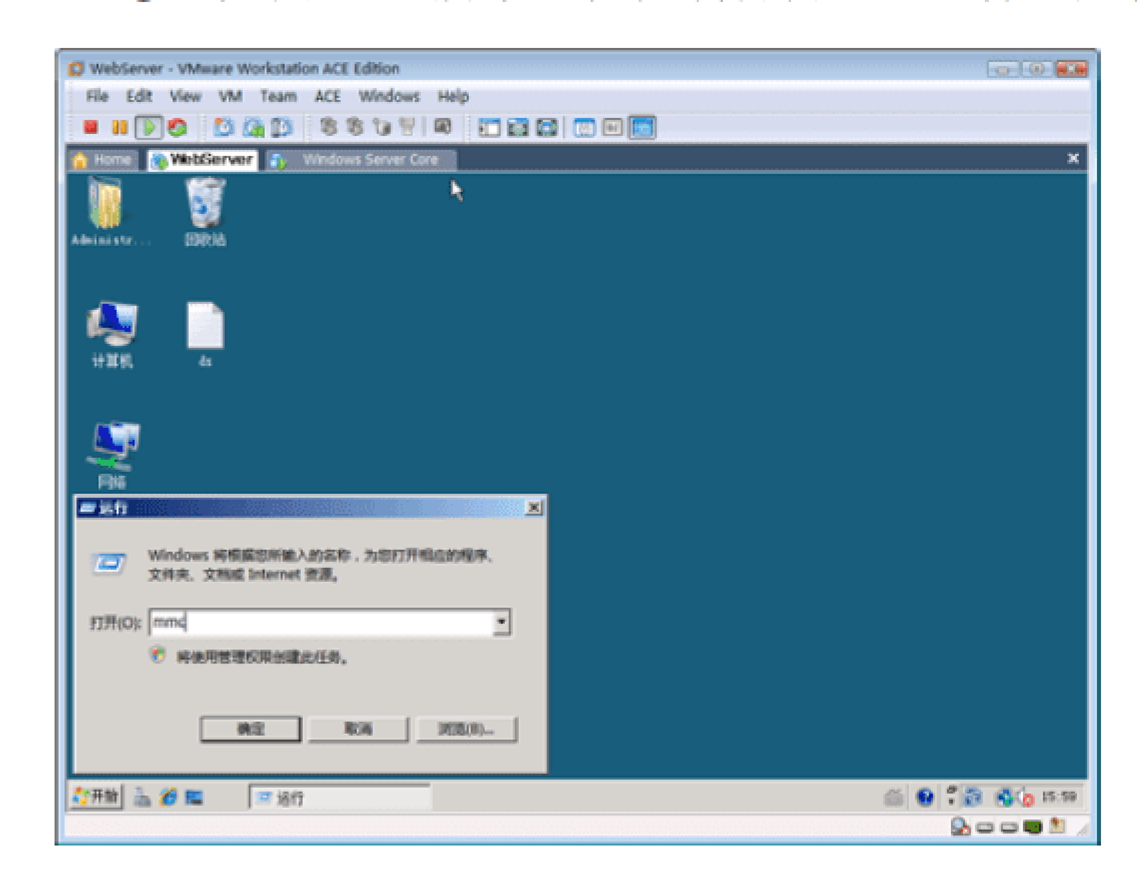


图 4-35　打开微软管理控制台

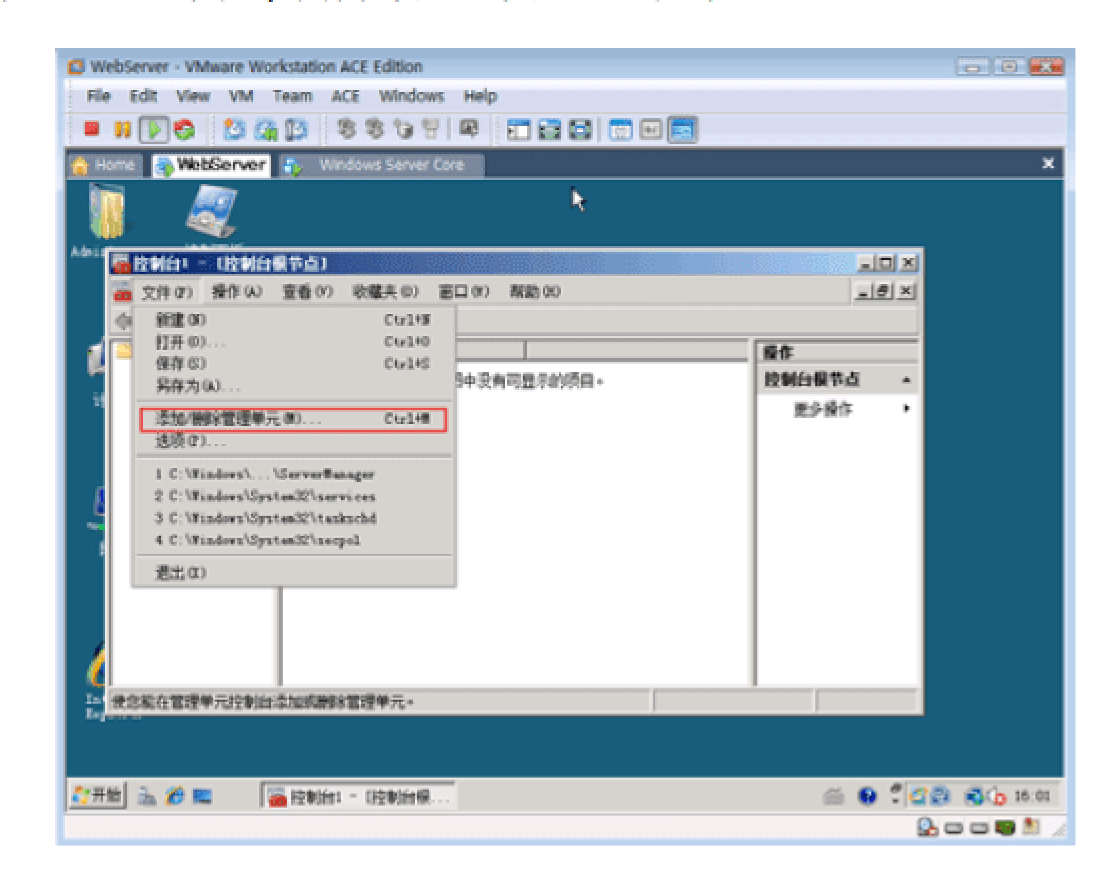


图 4-36　添加/删除管理单元

⑧ 如图 4-37 所示，在出现的“添加或删除管理单元”对话框中，选中“本地用户和组”选项，单击“添加”按钮。

⑨ 如图 4-38 所示，在出现的“选择目标机器”对话框中，选中“另一台计算机”单选按钮，输入 Windows Server Core 计算机的 IP 地址，单击“完成”按钮，最后单击“确定”按钮。

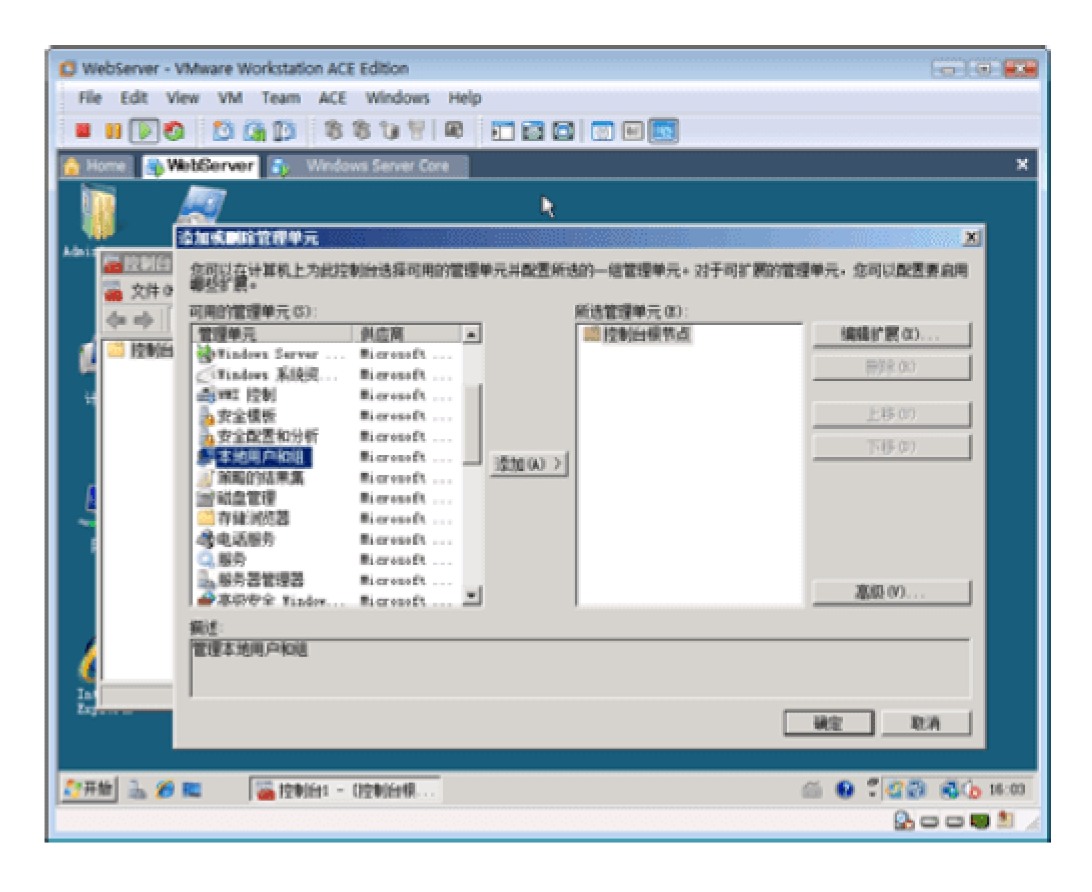


图 4-37　添加本地用户和组管理单元

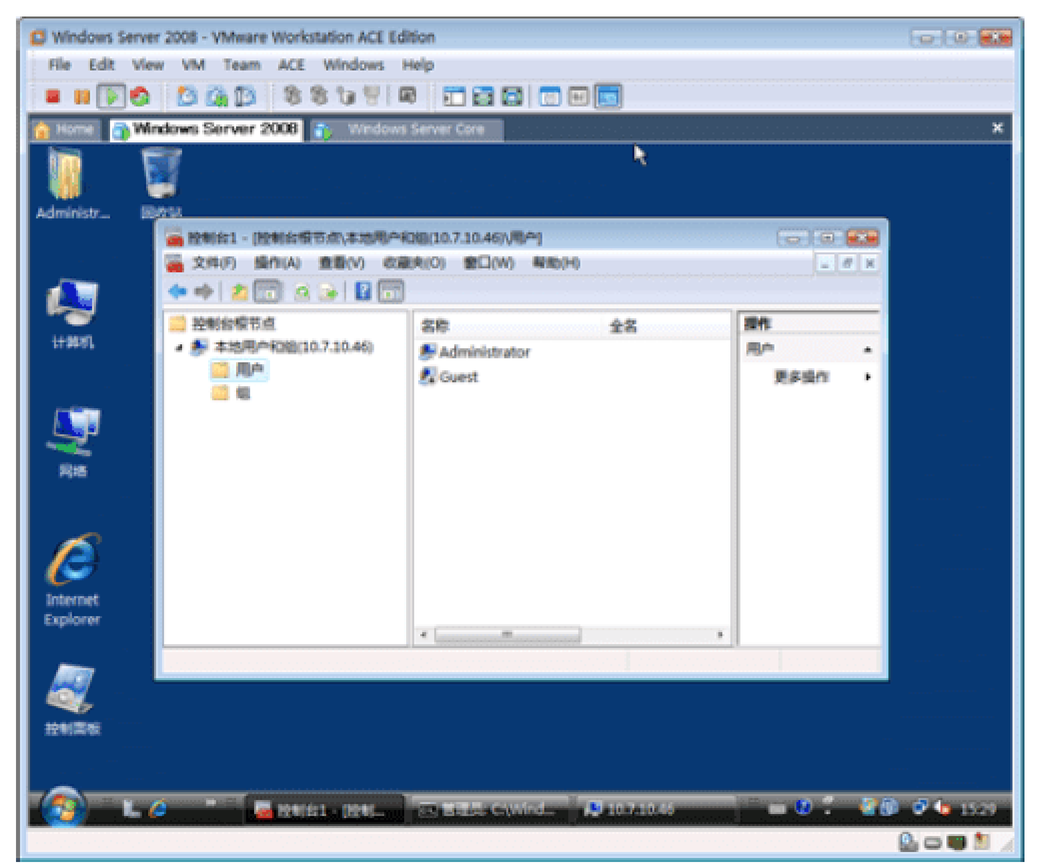
图 4-38　选择计算机

⑩ 如图 4-39 所示，此时该管理工具可以管理 Windows Server Core 服务器上的用户和组了。

⑪ 为了以后管理方便，可以将其保存，选择“文件”|“保存”命令，在打开的对话框中输入文件名

“Server Core 的用户和组”。以后单击该管理工具就能直接打开这个管理单元。

⑫ 在 MMC 同样可以添加更多的管理单元。如图 4-40 所示，添加了管理 Server Core 服务器的服务管理单元，可以管理 Server Core 上的服务。



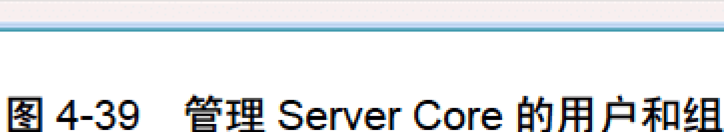


图 4-39　管理 Server Core 的用户和组

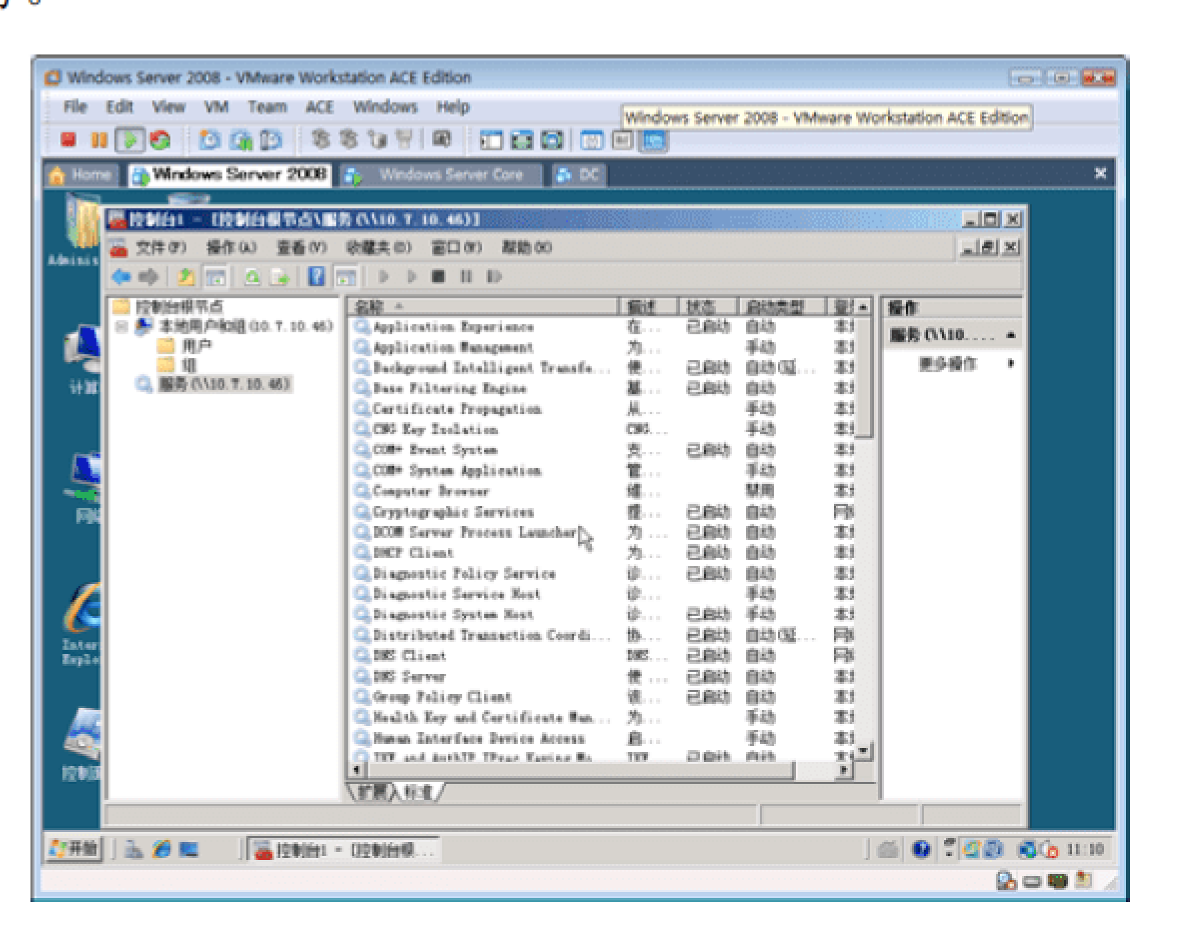


图 4-40　管理 Server Core 的服务

4.4　用户账户控制概述

用户账户控制 (UAC) 是 Windows Vista 和 Windows Server 2008 操作系统的一个新安全组件。UAC 使用户可以非管理员(在此版本的 Windows 中称为“标准用户”)以及管理员身份执行常见任务，而无须切换用户、注销或使用“以管理员身份运行”命令。标准用户账户与 Windows XP 中的用户账户类似。作为本地 Administrators 组成员的用户账户以标准用户身份运行大多数应用程序。因为 UAC 在进行操作时将用户功能和管理员功能分隔开来，所以它是此版本 Windows 的一个重要增强功能。

当管理员登录到 Windows Vista 或 Windows Server 2008 计算机时，将为用户分配两个单独的访问令牌。Windows 使用访问令牌(包含用户的组成员身份、授权数据和访问控制数据)控制用户可以访问的资源和任务。在先前版本的 Windows 中，管理员账户接收的一个访问令牌包含授予用户访问所有 Windows 资源权限的数据。此访问控制模型不包含任何故障保险检查，而故障保险检查可以确保用户真正执行需要他(或她)的管理访问令牌的任务。

因此，恶意软件可以将其自身安装在计算机上，而不会通知用户。此过程通常称为“无提示”安装。因为用户是管理员，所以恶意软件可以使用管理员的访问控制数据感染核心操作系统文件。在某些情况下，恶意软件可能会变得几乎不可能被删除，而且可能会造成更多破坏。

此版本的 Windows 中的标准用户和管理员之间的主要区别在于他们对计算机有多少控制权。管理员可以更改系统状态、关闭防火墙、关闭策略、安装影响计算机上每个用户的服务或驱动程序等，可以为整台计算机安装软件；而标准用户无法以这种方式更改系统状态。

4.4.1　为什么不应以管理员身份运行计算机

以 Administrators 组成员的身份运行计算机将使系统容易受到特洛伊木马及其他安全风险的威胁。

访问 Internet 站点或打开电子邮件附件的简单行为都可能破坏系统。不熟悉的 Internet 站点或电子邮件附件可能包含特洛伊木马代码，这些代码可以下载到系统并被执行。

如果以本地计算机的管理员身份登录，特洛伊木马可能使用管理访问权重新格式化用户的硬盘，删除文件并创建新的用户账户。

在本地计算机上，建议将域用户账户仅添加到 Users 组(而非 Administrators 组)，以执行例行任务，包括运行程序和访问 Internet 站点。当需要在本地计算机上执行管理任务时，应通过管理凭据使用“以管理员身份运行”启动程序。

可以使用“以管理员身份运行”完成管理任务，而不致将计算机置于不必要的风险中。

4.4.2 启用用户账户控制(UAC)

以管理员的身份登录计算机。

① 选择“开始”→“设置”→“控制面板”→“用户帐户”命令，打开如图 4-41 所示对话框，单击“打开或关闭用户帐户控制”按钮。



图 4-41　打开或关闭用户账户控制

② 如图 4-42 所示。选中“使用用户帐户控制(UAC)帮助保护您的计算机”复选框。

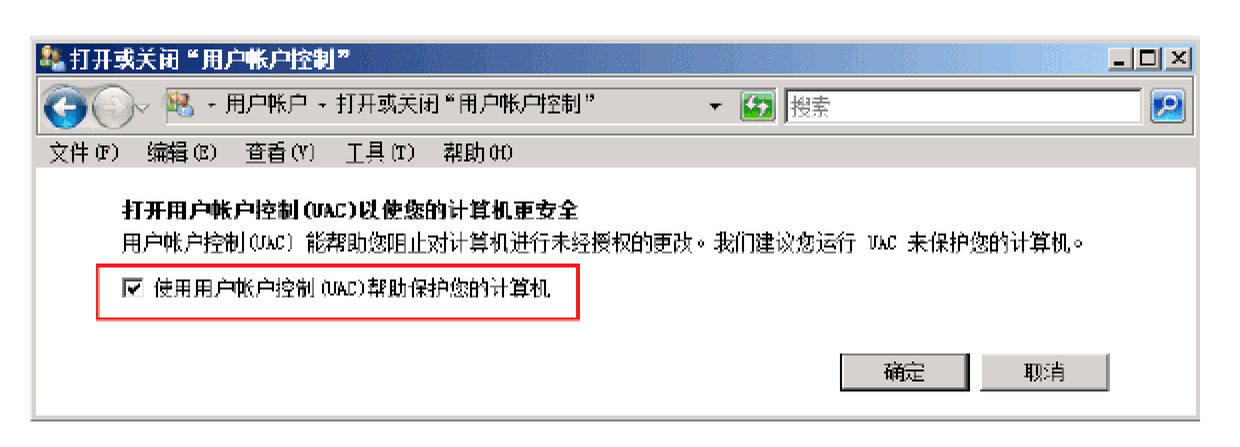


图 4-42　启用用户账户控制

4.4.3 以管理员身份运行

以普通用户的账户登录计算机。单击“服务器管理器”开始按钮，出现“用户帐户控制”对话框，如图 4-43 所示，会显示这台计算机上具有管理员权限的账户，单击账户，输入密码，单击“确定”按钮，就可以管理员的身份打开服务器管理器了。

另外，选择“开始”→“设置”→“控制面板”→“管理工具”命令，在打开的对话框中右击某个管理工具，在弹出的快捷菜单中选择“以管理员身份运行”命令，也可以管理员的身份打开服务器管理器，

如图 4-44 所示。

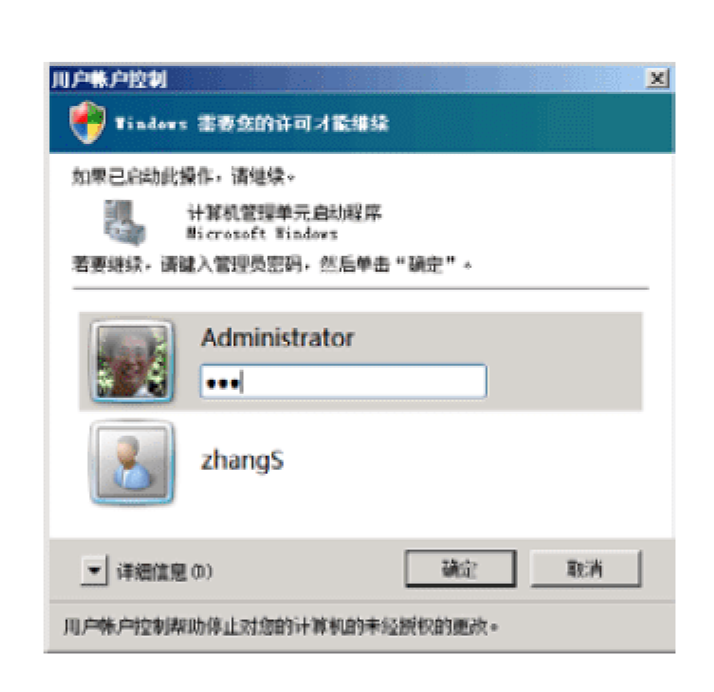


图 4-43　以管理员身份运行(一)

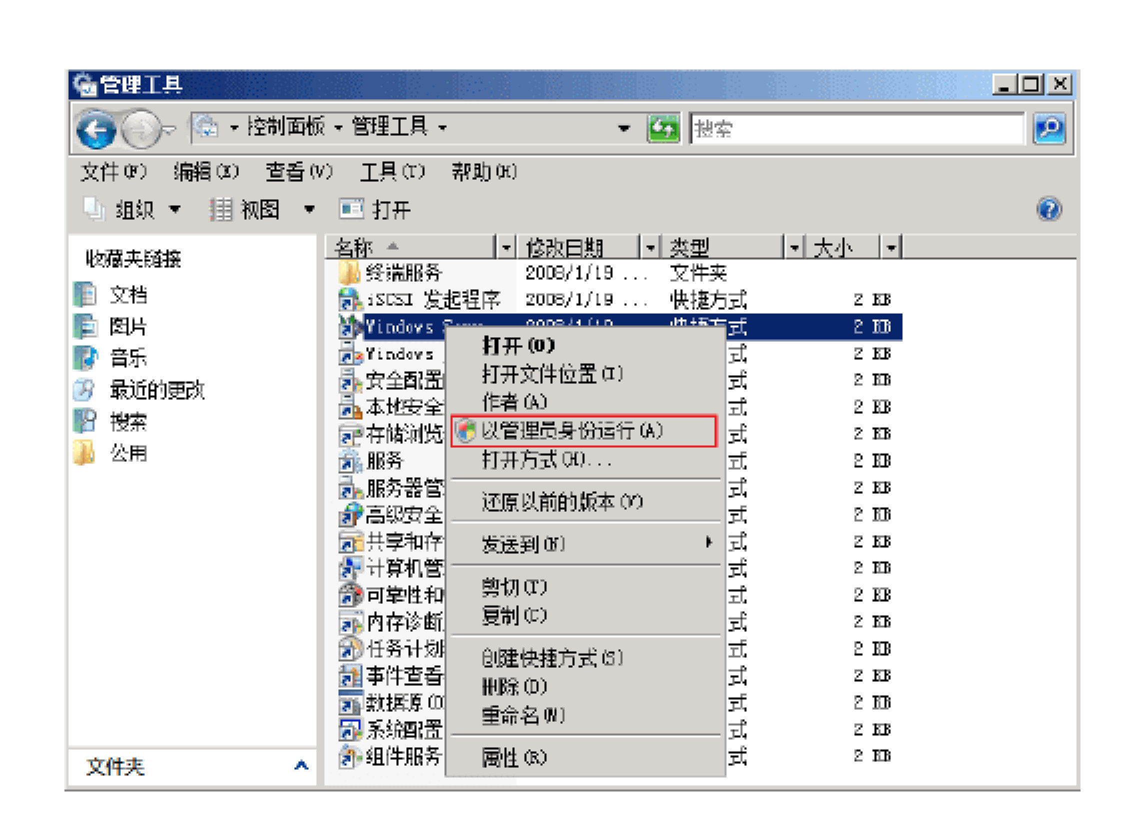


图 4-44　以管理员身份运行(二)

4.5　本地用户和组最佳实践

作为安全性的最佳实践，建议不要使用管理凭据登录到计算机。

未使用管理凭据登录到计算机时，可以使用“以管理员身份运行”来完成比标准用户账户更高级别权限的任务。

若要进一步保护本地计算机，建议遵循下列安全指南。

- 限制 Administrators 组中的用户数量。因为本地计算机中 Administrators 组的成员拥有对该计算机的完全控制权限。
- 禁用 Guest 账户。Guest 账户由在这台计算机上没有实际账户的人使用。Guest 账户不要求密码，因此存在安全隐患。默认情况下将禁用 Guest 账户，并且建议将其保持禁用状态。
- 禁用 Administrator 账户。默认情况下将禁用 Administrator 账户，并且建议将其保持禁用状态。
- 分配给特定默认本地组的某些默认用户权限可能允许这些组的成员获得计算机的额外权限，包括管理权限。因此，必须信任属于 Administrators 和 Backup Operators 组的所有人员。



注意：如果你位于包含运行 Windows 95 和 Windows 98 的计算机的网络上，请使用不超过 14 个字母的密码。

- 可以创建包含多达 127 个字符的密码。但是，运行 Windows 95 和 Windows 98 的计算机仅支持不超过 14 个字符的密码。如果密码超过 14 个字符，则可能无法从运行 Windows 95 和 Windows 98 的计算机登录到网络。

第 5 章　Windows Server 2008 活动目录

计算机的组织形式包括工作组和域两种，工作组中的计算机没有办法集中管理，用户访问网络资源也没有办法统一身份验证，而将计算机组织成域环境，可以实现集中管理域中的计算机和域用户，以及实现集中的身份验证。

在活动目录中域用户的配置文件即用户的环境可以放到网络中的一个服务器的共享文件夹中，用户在域中任何一台计算机登录，都能使用自己的环境。

在活动目录中使用组的策略：A→G→DL→P 策略。

关键词

- 活动目录介绍
- 创建 Windows Server 2008 活动目录域
- 设计活动目录组织单位
- 创建和管理域用户
- 漫游式用户配置文件
- 在活动目录中使用组

5.1 活动目录介绍

下面介绍计算机的两种组织形式：工作组和域。先介绍工作组的限制，再介绍活动目录的功能，也就是将计算机组织成域的形式，从而解决工作组面临的难题。

5.1.1 工作组中的限制

计算机安装操作系统后，默认的计算机属于 Workgroup 工作组。工作组是最简单的计算机组织形式。

工作组中的计算机没有统一的管理机制，每台计算机的管理员只能管理本地计算机，比如设置计算机的安全策略、本地连接和共享等管理工作。

工作组的计算机也没有对用户账户的统一身份验证机制，用户登录计算机只能使用该计算机的本地用户账户，由本地计算机来验证用户的身份。当访问网络上的共享资源时，还需要提供访问网络资源的凭据。用户需要记下访问各个服务器的账户和密码。

工作组的计算机也没有统一查找网络资源的机制，比如网络中的共享打印机、企业的用户账户信息及共享文件夹等。

基于以上限制，工作组是较小规模计算机网络组织的形式。在大企业中网络规模大，计算机数量多，需要统一的管理和集中的身份验证，并且能够给用户提供方便的搜索和使用网络资源的方式，工作组的组织形式就不适合了。

5.1.2 活动目录的功能

先明确域的概念。

- 将网络中多台计算机逻辑上组织到一起，进行集中管理，这种区别于工作组的逻辑环境叫做域。
- 域是组织与存储资源的核心管理单元。

活动目录提供了存储网络上对象信息并使网络用户使用该数据的方法。活动目录有以下特点。

- 集中管理。
- 便捷的网络资源访问。
- 用户一次登录就可访问整个网络资源。
- 网络资源主要包含用户账户、组、共享文件夹、打印机等。
- 可扩展性。

5.1.3 DNS 服务器在域环境中的作用

ADDS 服务器角色要求域名系统 (DNS) 服务按名称查找计算机、域控制器、成员服务器和网络服务。DNS 服务器角色通过将名称映射到 IP 地址为基于 TCP/IP 的网络提供 DNS 名称解析服务，从而使计算机可以查找 ADDS 环境中的网络资源。

- 域名解析：DNS 服务器通过其 A 记录将域名解析为 IP 地址。

- 定位活动目录服务：客户机通过 DNS 服务器上 SRV 记录定位目录服务。

通常情况下，DNS 和 DC 两个服务装在同一台计算机上。客户机如果想要找到域控制器，其 DNS 必须指向域控制器上的 DNS。

5.2 实战：创建 Windows Server 2008 域

任务描述

下面将创建如下域环境。

- DCServer 作为域控制器和 DNS 服务器，服务器为 FileServer，Research 是研发部门的计算机，Sales 是销售部门的计算机。
- HanLG 是研发部门的用户账户，ZhangJL 是研发部门的归档账户，WangRS 是销售部门的用户账户。
- FielServer 存放用户的配置文件，共享公司共享文件夹“研发图纸”和“销售资料”。
- ProfileServer 存放域用户漫游用户配置文件。

实战环境

如图 5-1 所示。

- DCServer 安装了 Windows Server 2008 企业版操作系统，IP 地址为 10.7.10.12。
- FileServer 安装了 Windows Server 2008 企业版操作系统。
- Research 安装了 Windows Server 2008 企业版操作系统。
- ProfileServer 安装 Windows Server 2008 企业版核心。
- Sales 安装了 Vista 操作系统。

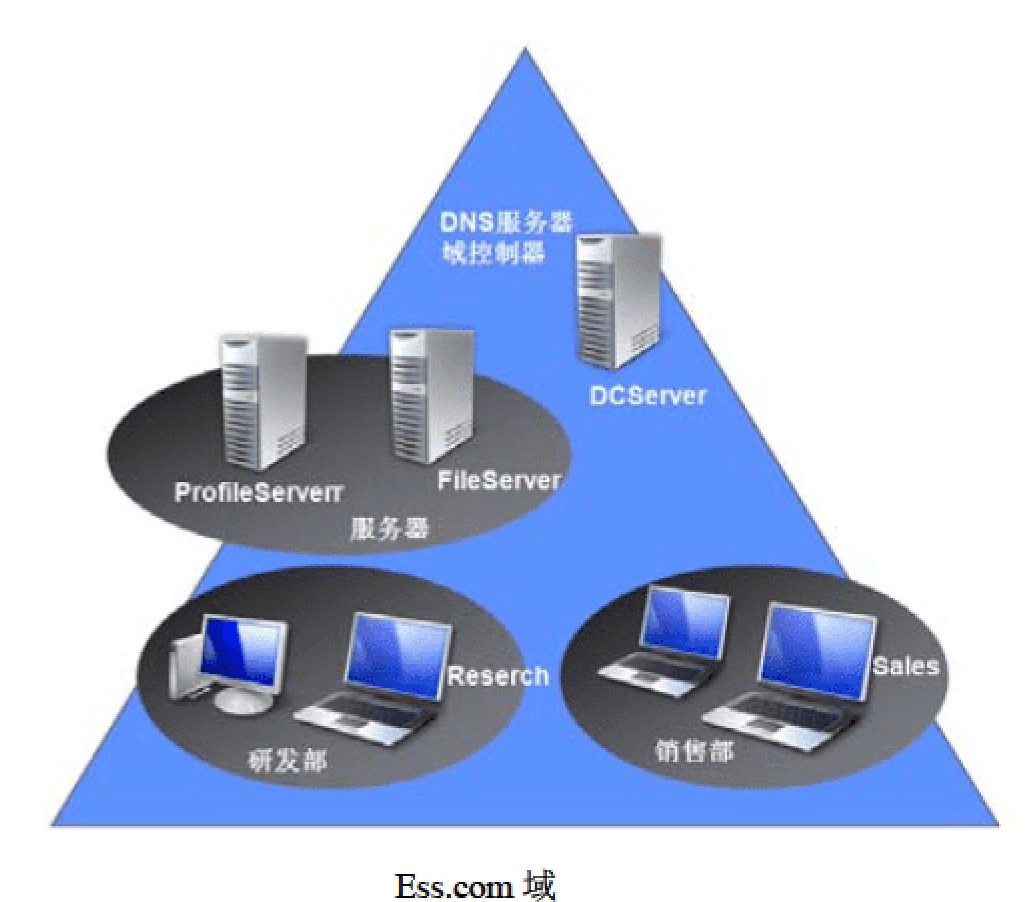


图 5-1 实战环境

实战目标

- 学会在 Windows Server 2008 企业版操作系统中安装活动目录。
- 安装活动目录后的检查。

- 学会将计算机加入域。
- 能够根据部门结构在活动目录中创建组织单元。
- 创建和管理域用户。
- 在域环境中使用组。
- 创建漫游式用户配置文件。

该实战中用到了以下虚拟机，如图 5-2 所示，选择 VM→Settings 命令，在打开的 Virtual Machine Settings 对话框中，切换到 Options 选项卡，在 Virtual machine name 文本框中输入虚拟机的名称。

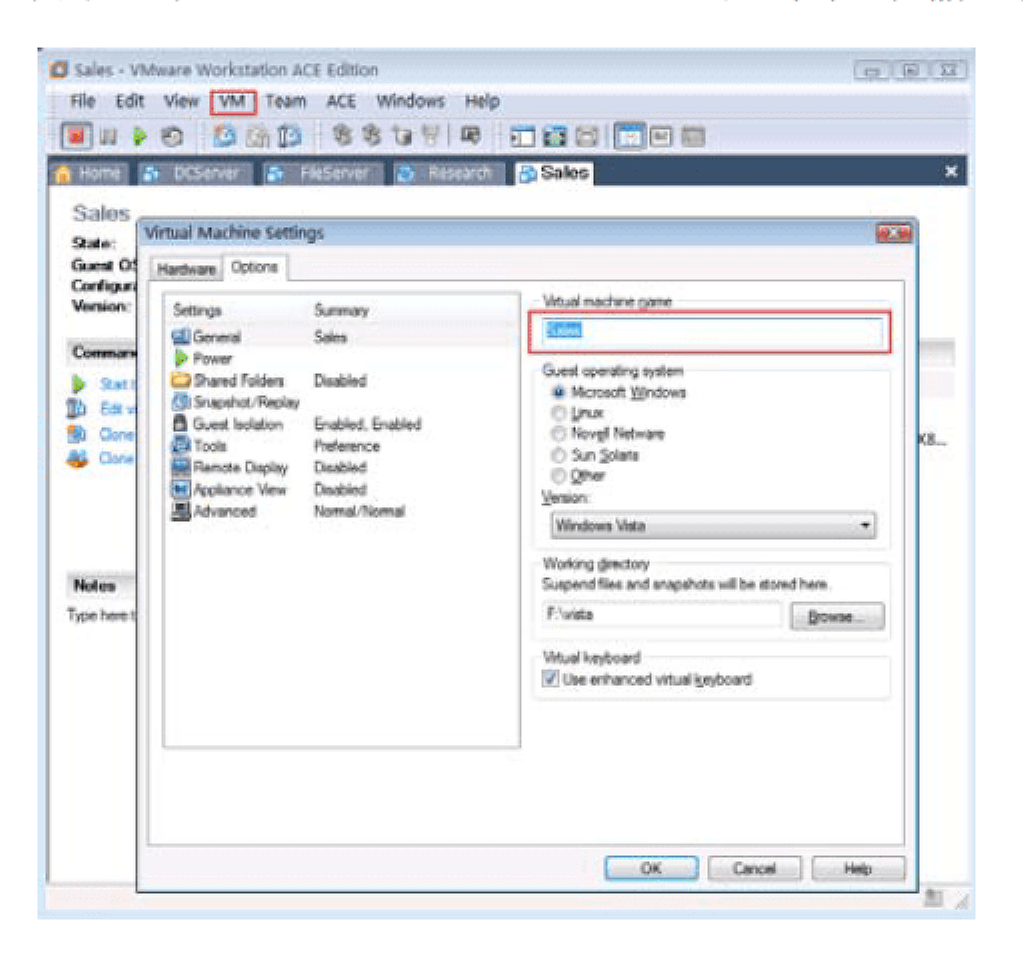


图 5-2 设置虚拟机显示名

5.2.1 在 DCServer 上安装活动目录

1. 任务

- 更改计算机名称。
- 更改 IP 地址。
- 安装活动目录。

2. 步骤

① 以管理员的身份登录 DCServer，更改计算机名为 DCServer，重启操作系统。

② 如图 5-3 所示，将 DCServer 的 IP 地址配置为静态 IP 地址 10.7.10.12，子网掩码为 255.255.255.0，默认网关为 10.7.10.1，首选 DNS 服务器 10.7.10.12。因为安装活动目录的同时也要安装 DNS 服务，DNS 服务要求服务器使用静态 IP 地址。

③ 选择“开始”→“运行”命令，在打开的对话框中输入 dcpromo，单击“确定”按钮。如图 5-4 所示，打开活动目录安装向导，单击“下一步”按钮。

④ 如图 5-5 所示，在“操作系统兼容性”界面中，单击“下一步”按钮。

⑤ 如图 5-6 所示，在出现的“选择某一部署配置”界面中，选中“在新林中新建域”单选按钮，单击“下一步”按钮。

⑥ 如图 5-7 所示。在出现的“命名林根域”界面中，输入目录林根级域的完全限定域名(FQDN)ESS.COM，单击“下一步”按钮。

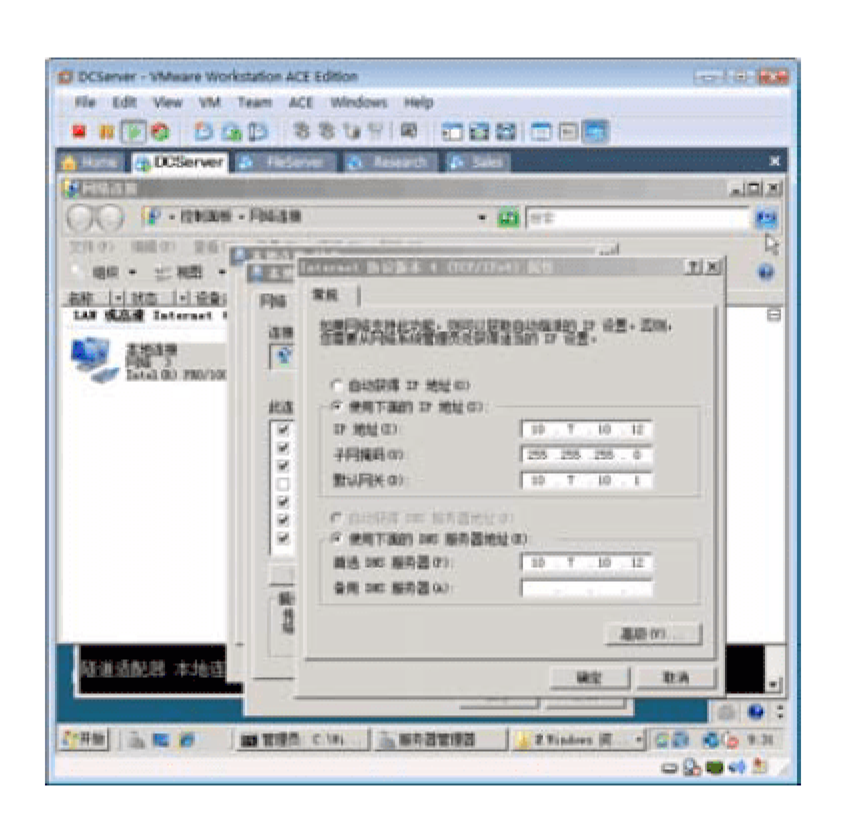


图 5-3　更改 IP 地址

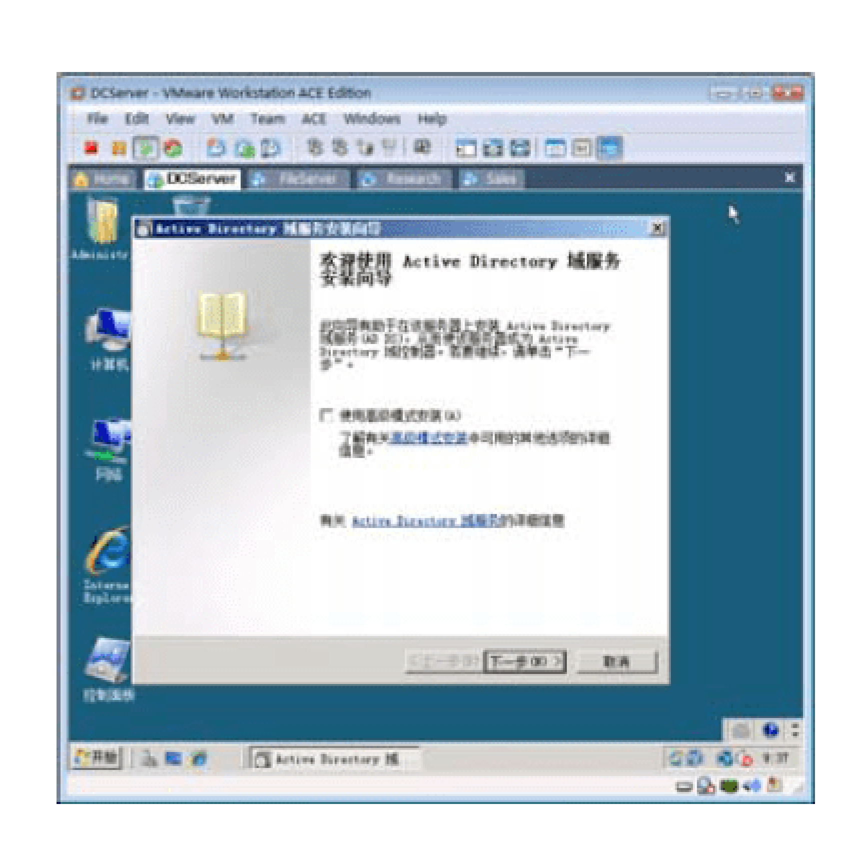


图 5-4　安装活动目录向导

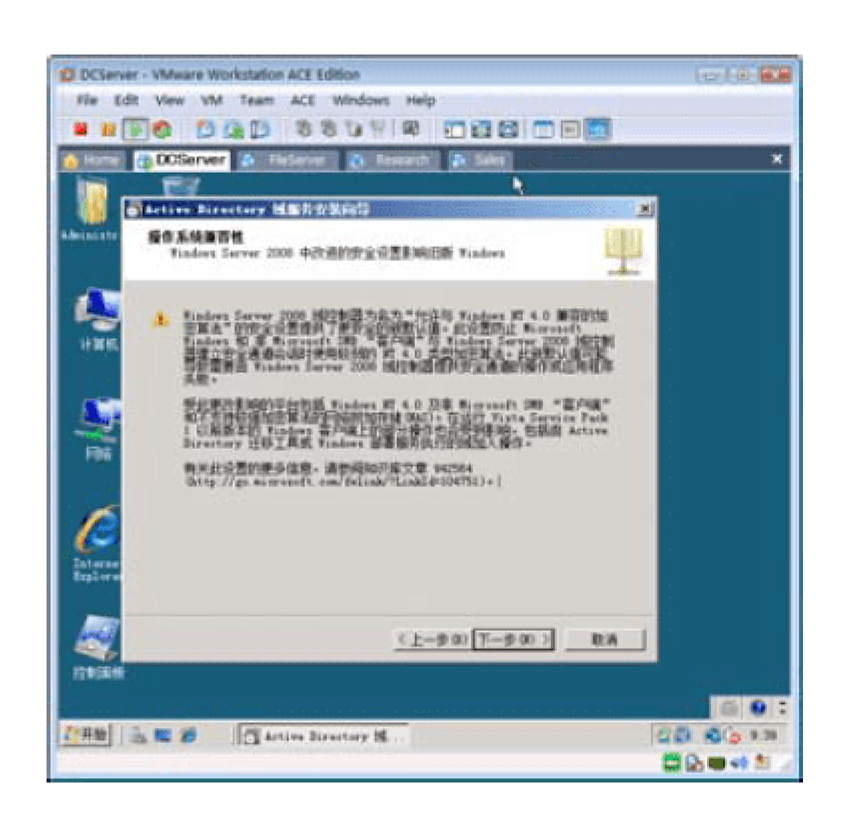


图 5-5　操作系统兼容性

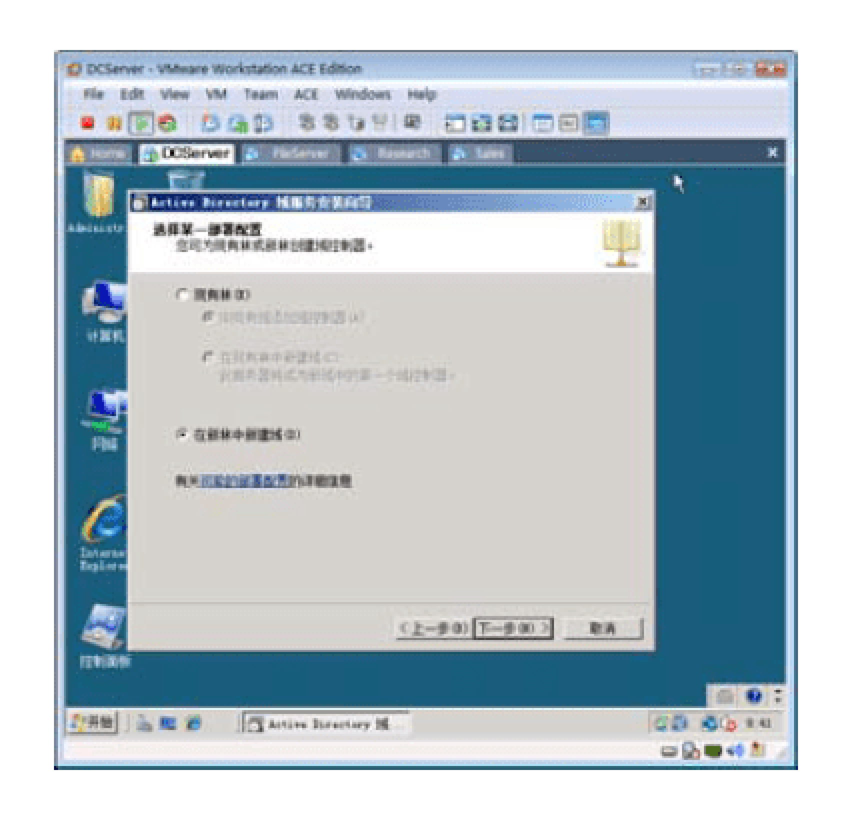


图 5-6　创建新的林

注：输入的域名要求是 FQDN 名字，不能是类似于 ESS 这样的名字。比如微软公司要创建一个域，域名可以输入 microsoft.com，但不能是 Microsoft。

⑦ 如图 5-8 所示，在出现的“设置林功能级别”界面中，选中 Windows Server 2008 选项，单击“下一步”按钮。

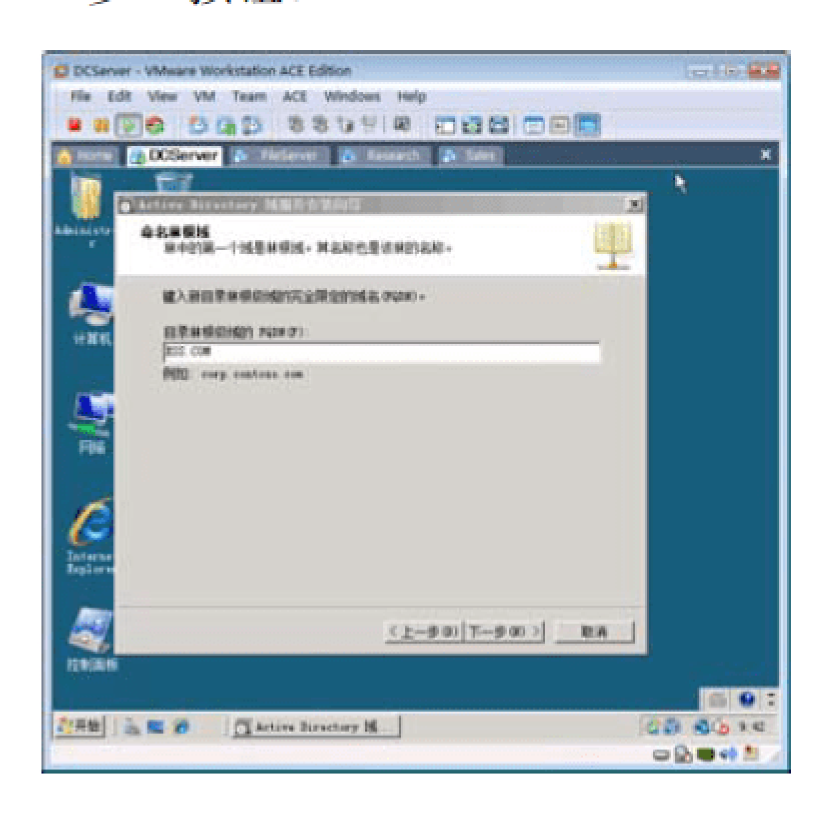


图 5-7　命名林根域

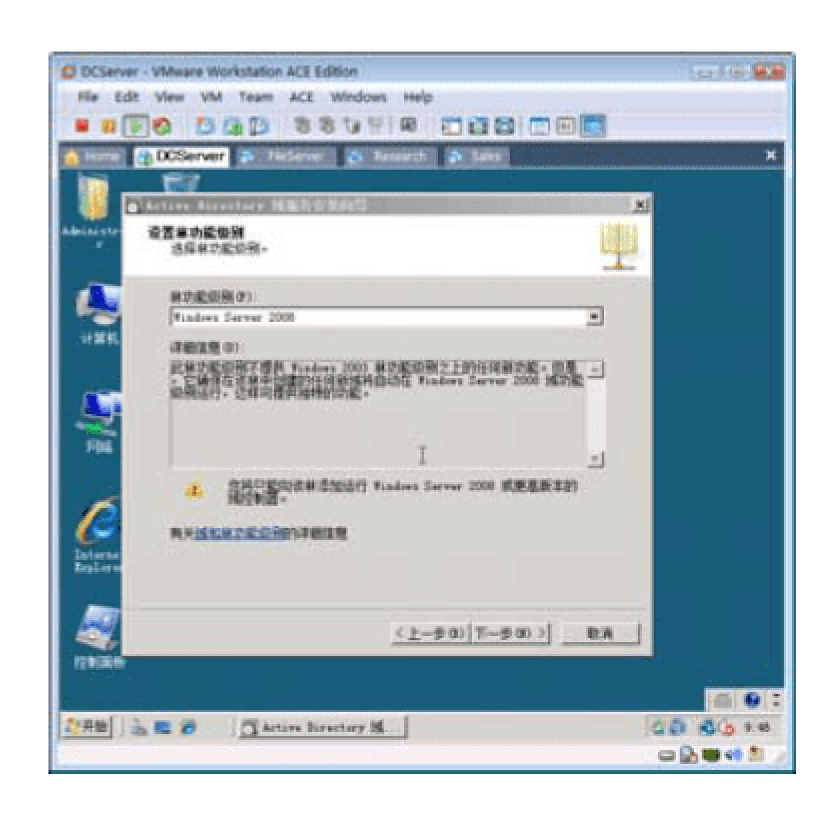


图 5-8　设置林功能级别

⑧ 如图 5-9 所示，在“其他域控制器选项”界面中，选中“DNS 服务器”复选框，单击“下一步”按钮。

注意：此林功能级别不提供 Windows 2003 林功能级别之上的任何新功能。但是，它确保在该林中创建的任何新域将自动在 Windows Server 2008 域功能级别运行，这样可提供独特的功能。

⑨ 如图 5-10 所示，在出现的提示对话框中，单击“是”按钮。

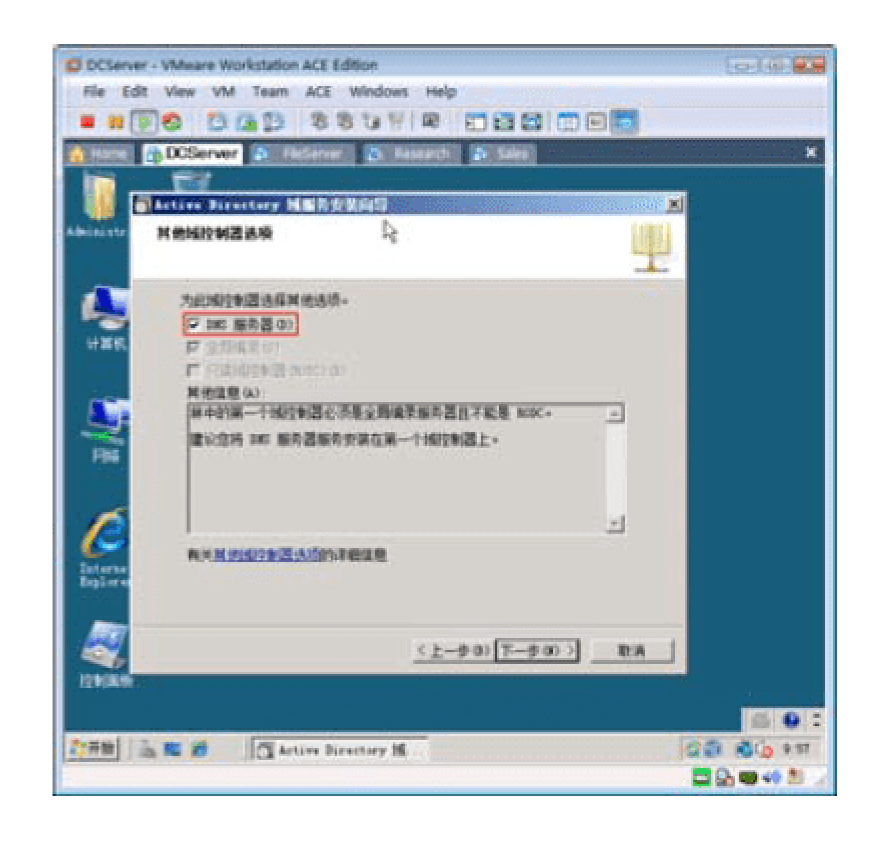


图 5-9 “其他域控制器选项”对话框

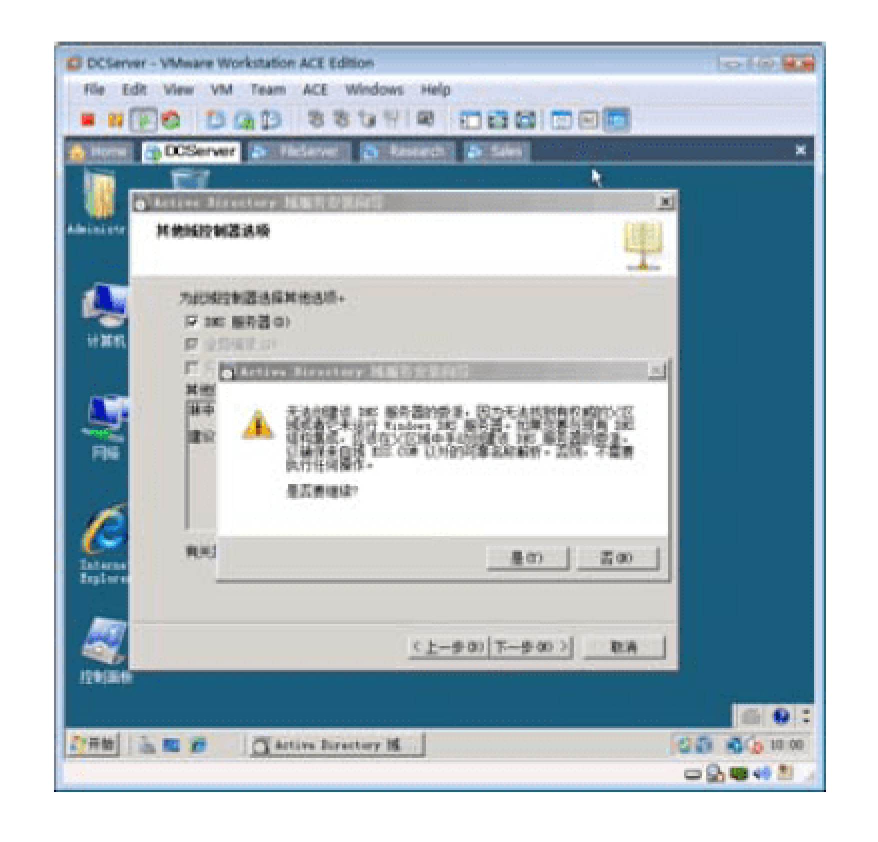
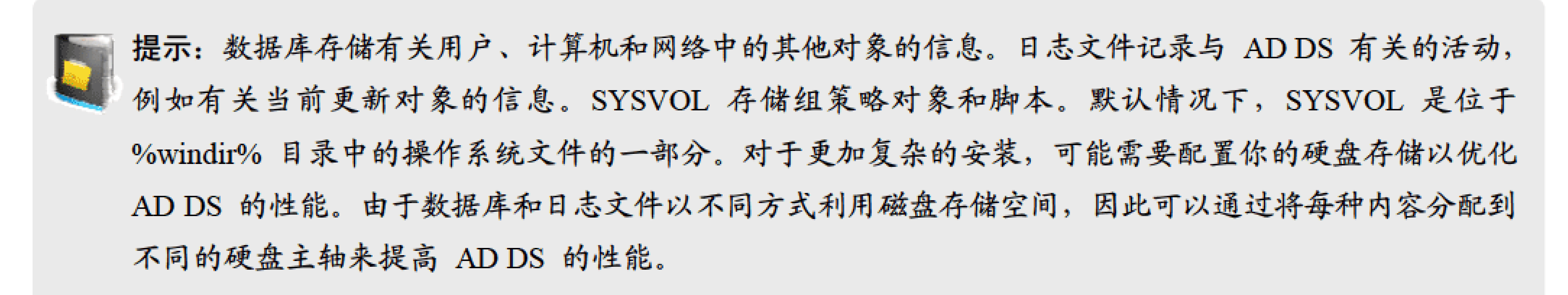


图 5-10 提示对话框

⑩ 如图 5-11 所示，在出现的“数据库、日志文件和 SYSVOL 的位置”界面中，指定数据库、日志文件和 SYSVOL 的位置，单击“下一步”按钮。



提示：数据库存储有关用户、计算机和网络中的其他对象的信息。日志文件记录与 AD DS 有关的活动，例如有关当前更新对象的信息。SYSVOL 存储组策略对象和脚本。默认情况下，SYSVOL 是位于 %windir% 目录中的操作系统文件的一部分。对于更加复杂的安装，可能需要配置你的硬盘存储以优化 AD DS 的性能。由于数据库和日志文件以不同方式利用磁盘存储空间，因此可以通过将每种内容分配到不同的硬盘主轴来提高 AD DS 的性能。

⑪ 如图 5-12 所示，在“目录服务还原模式的 Administrator 密码”界面中，输入活动目录恢复时用到的管理员密码，单击“下一步”按钮。

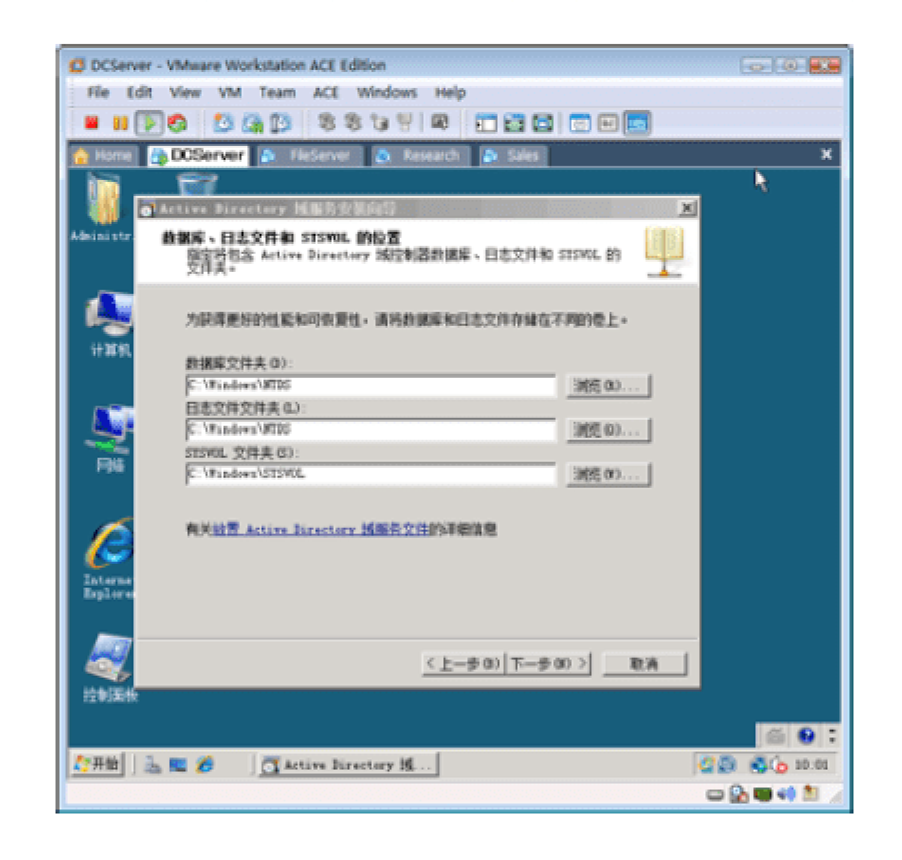


图 5-11 指定数据库、日志文件以及 SYSVOL 的位置

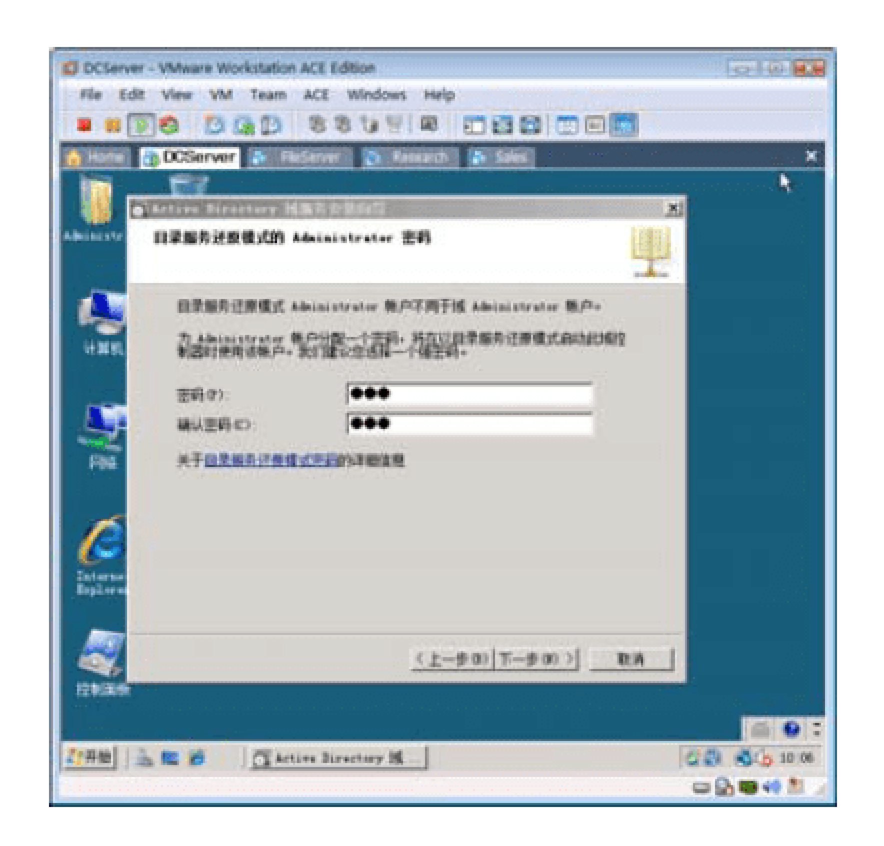


图 5-12 指定活动目录还原密码



提示：该密码在活动目录恢复时会用到，必须牢记，否则不能还原活动目录。

⑫　如图 5-13 所示，单击“下一步”按钮，在出现的对话框中选中“完成之后重启”复选框完成向导。



提示：在 Active Directory 域服务(AD DS)未运行(因为 AD DS 已停止或因为域控制器已在 DSRM 中启动)时，目录服务还原模式(DSRM)密码是登录域控制器所必需的。

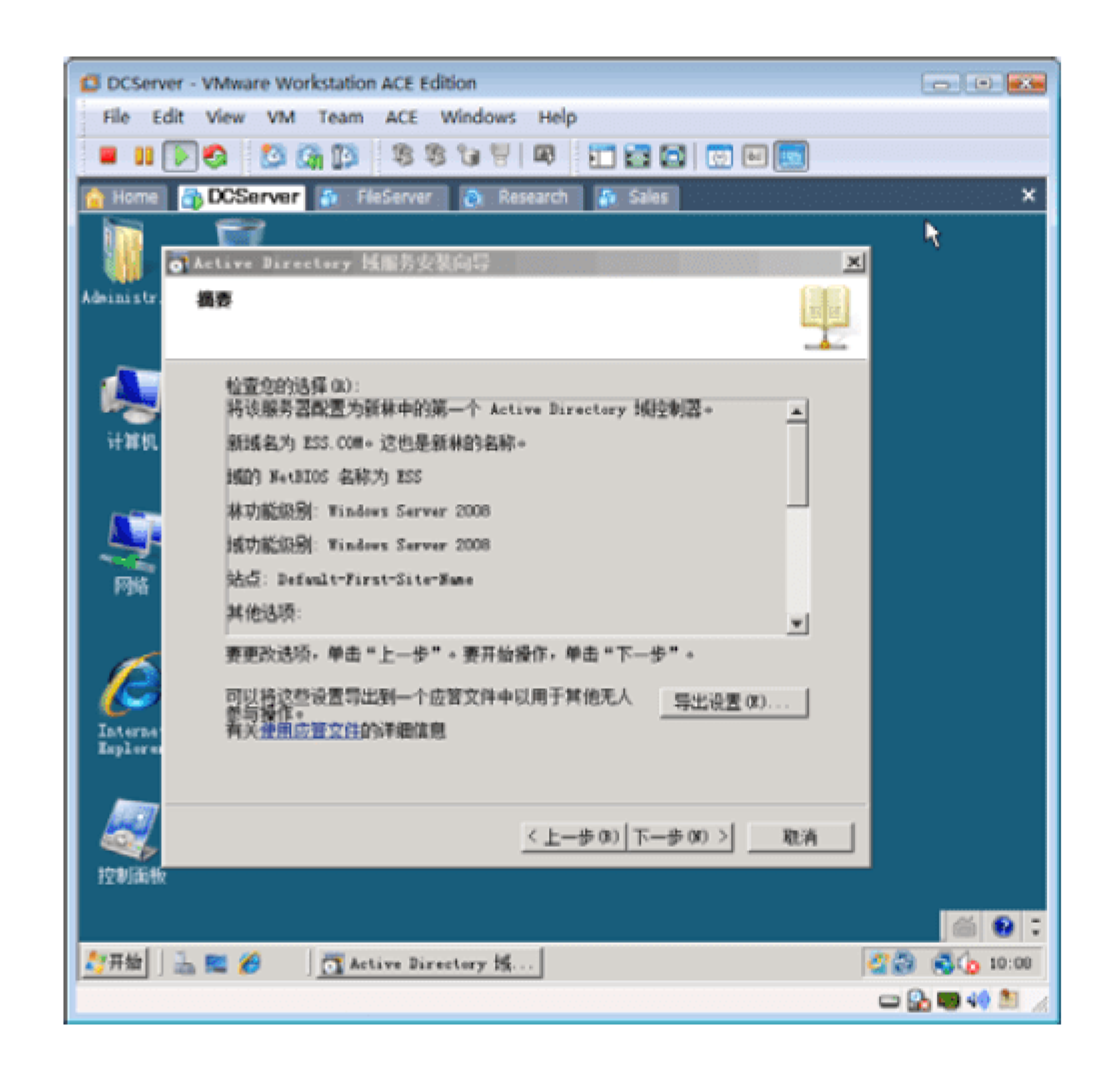


图 5-13　摘要



注意：卸载活动目录也是用 dcpromo 命令。安装上活动目录后，本地用户和组将不可用。

5.2.2　安装后的检查

1. 任务

- 检查活动目录安装是否正常。
- 更改域控制器本地连接的 DNS 设置。
- 检查 DNS 服务域控制器注册的 SRV 记录。

2. 步骤

①　以管理员身份登录到域控制器。

②　如图 5-14 所示，更改域控制器使用的 DNS 服务器，打开 TCP/IPv4 协议，将首选的 DNS 服务器更改为 10.7.1.110。

注意：默认安装活动目录后，首选 DNS 会指定成 127.0.0.1，所以启动后的第一件事就是将首选的 DNS 指向自己的 IP 地址。

③　如图 5-15 所示，打开服务管理器，检查 DNS 上的 SRV 记录。注意上面是 4 项，下面是 6 项。

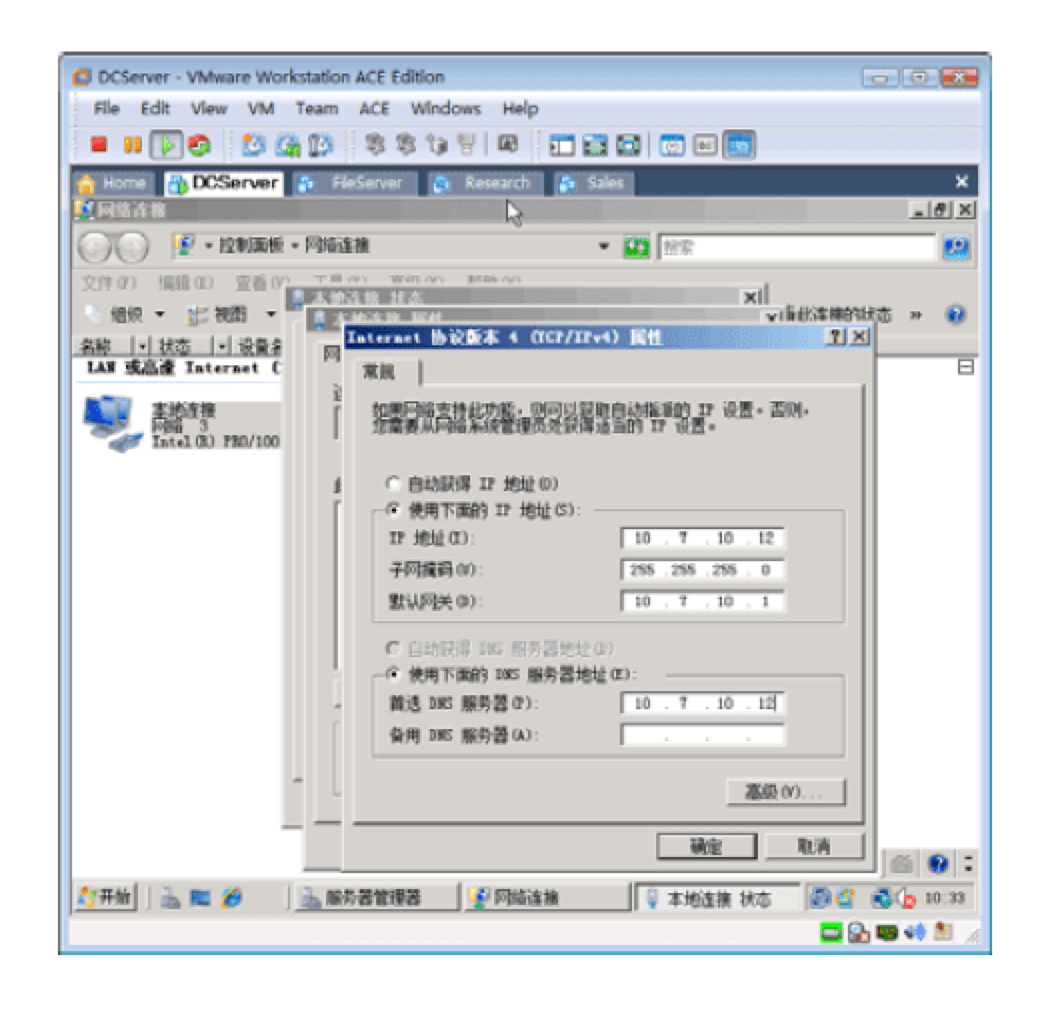




图 5-14　将首选的 DNS 指向本机的 IP 地址

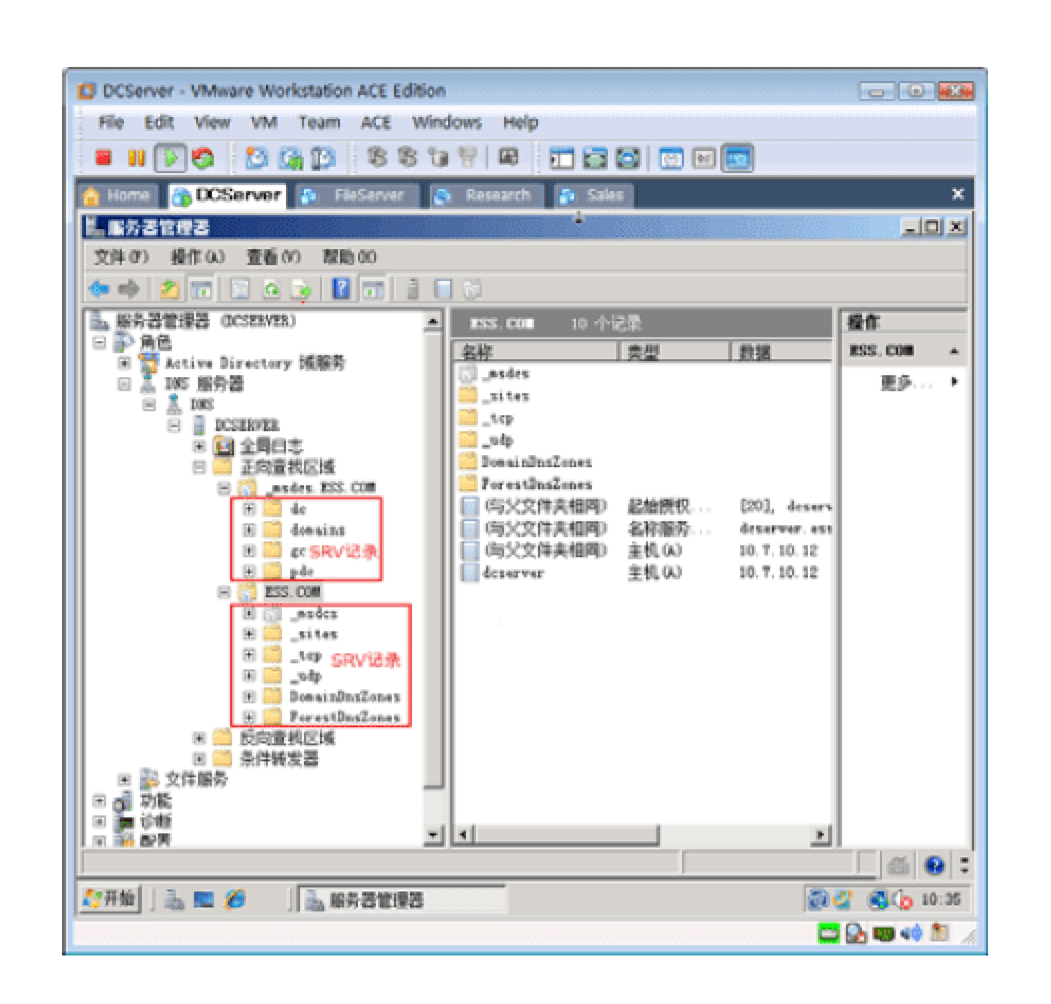


图 5-15　域控制器项 DNS 注册的 SRV 记录



提示：这些 SRV 记录是域控制器注册的。通过这些记录，客户机能够找到 ESS.COM 这个域的域控制器。如果安装完活动目录后，发现 SRV 记录不全，则客户端就无法找到域控制器。如何做呢？请看下面的任务。

④　检查活动目录的默认结构。在服务器管理器中，展开“角色”→“Active Directory 域服务”→“Active Directory 用户和计算机”→ESS.COM 节点，如图 5-16 所示。

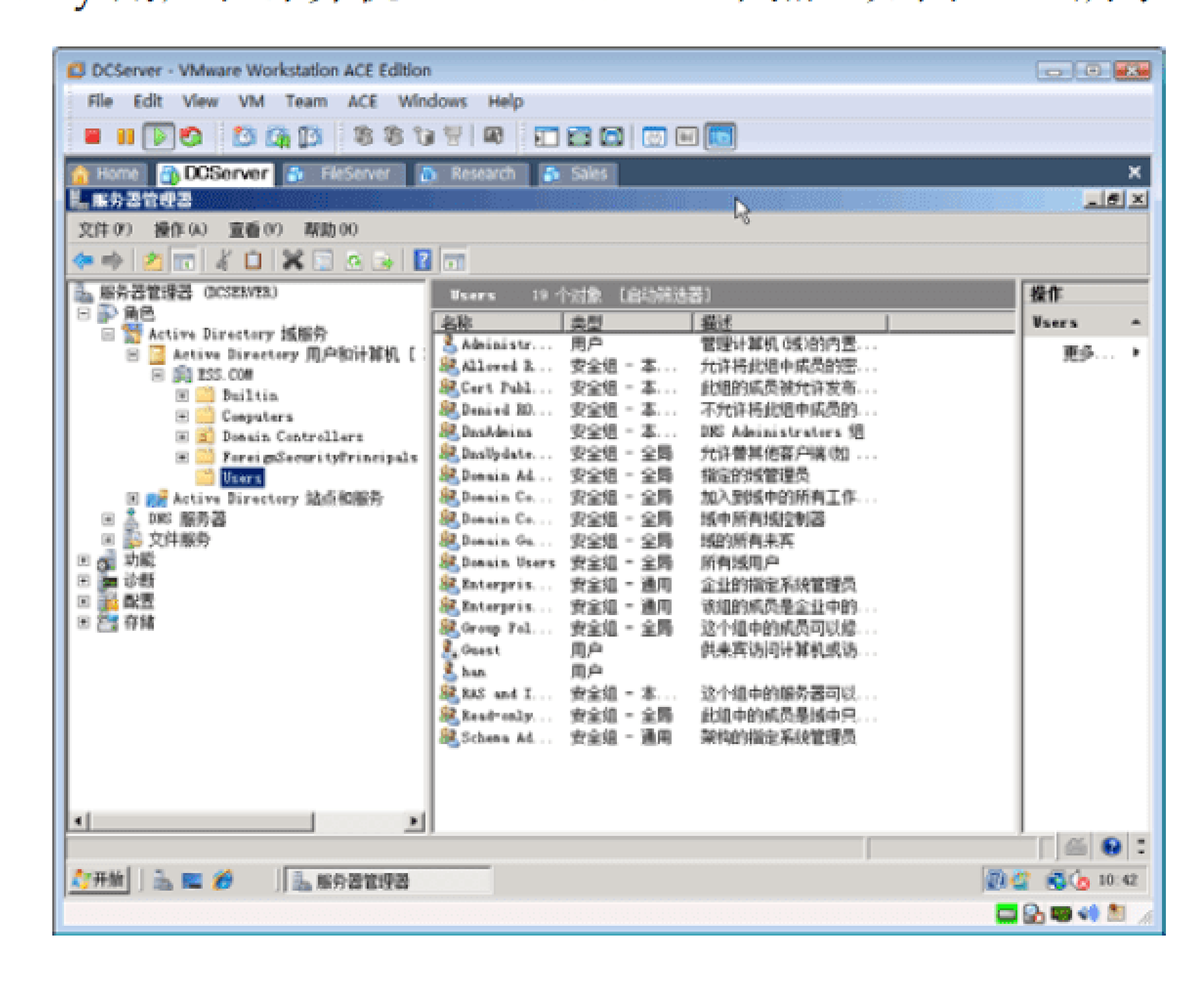
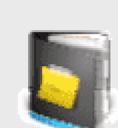


图 5-16　活动目录默认结构

- Builtin：存放的是内置的组。
- Computers：默认计算机加入域后，计算机账户存放的位置就是 Computers。
- Domain Controllers：存放该域中的域控制器，不要轻易将域控制器移动到其他位置。
- ForeignSecurityPrincipals：存放信任的外部域中安全主体。
- Users：默认用户的存放位置。

⑤　如图 5-17 所示，选中 ESS.COM 选项，选择“查看”→“高级功能”命令。

⑥　如图 5-18 所示，可以看到活动目录中更多容器。



提示：启用高级功能后能够看到隐藏的系统目录。

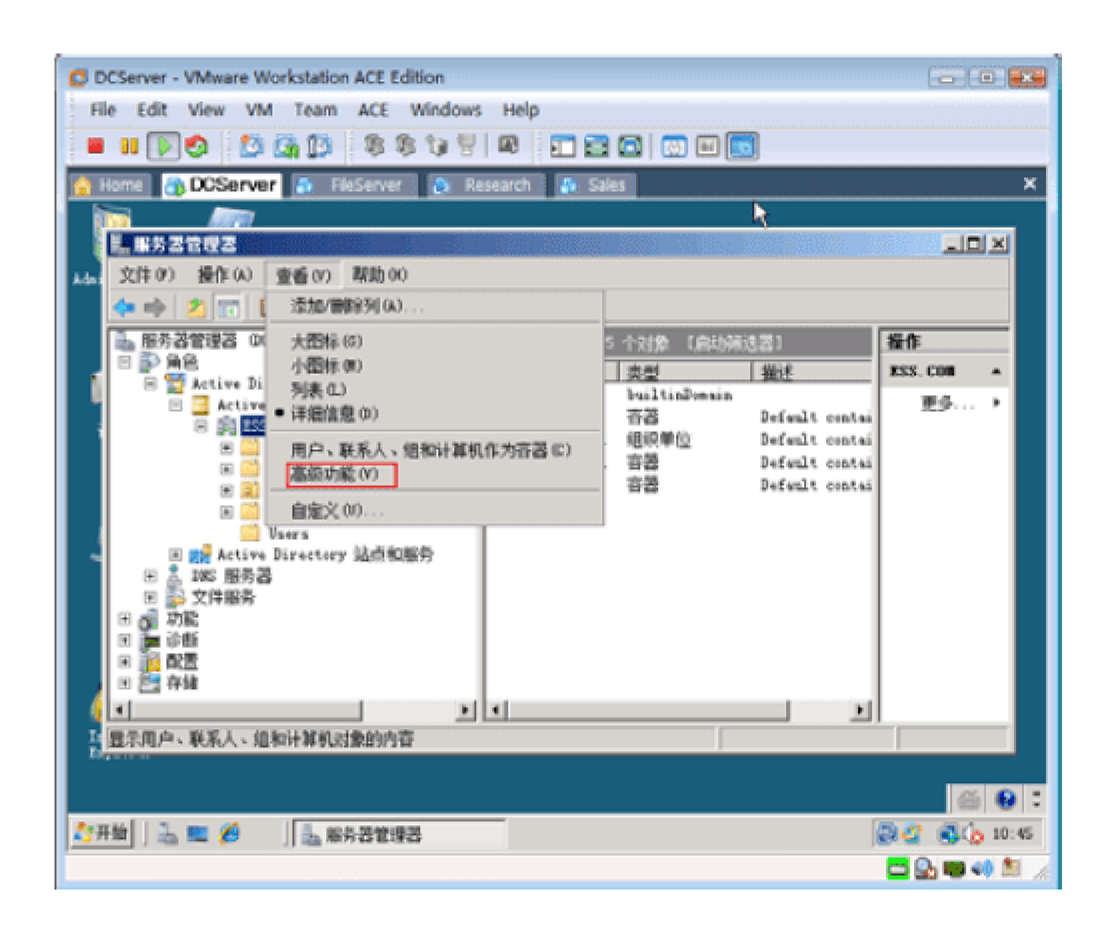




图 5-17　启用高级功能

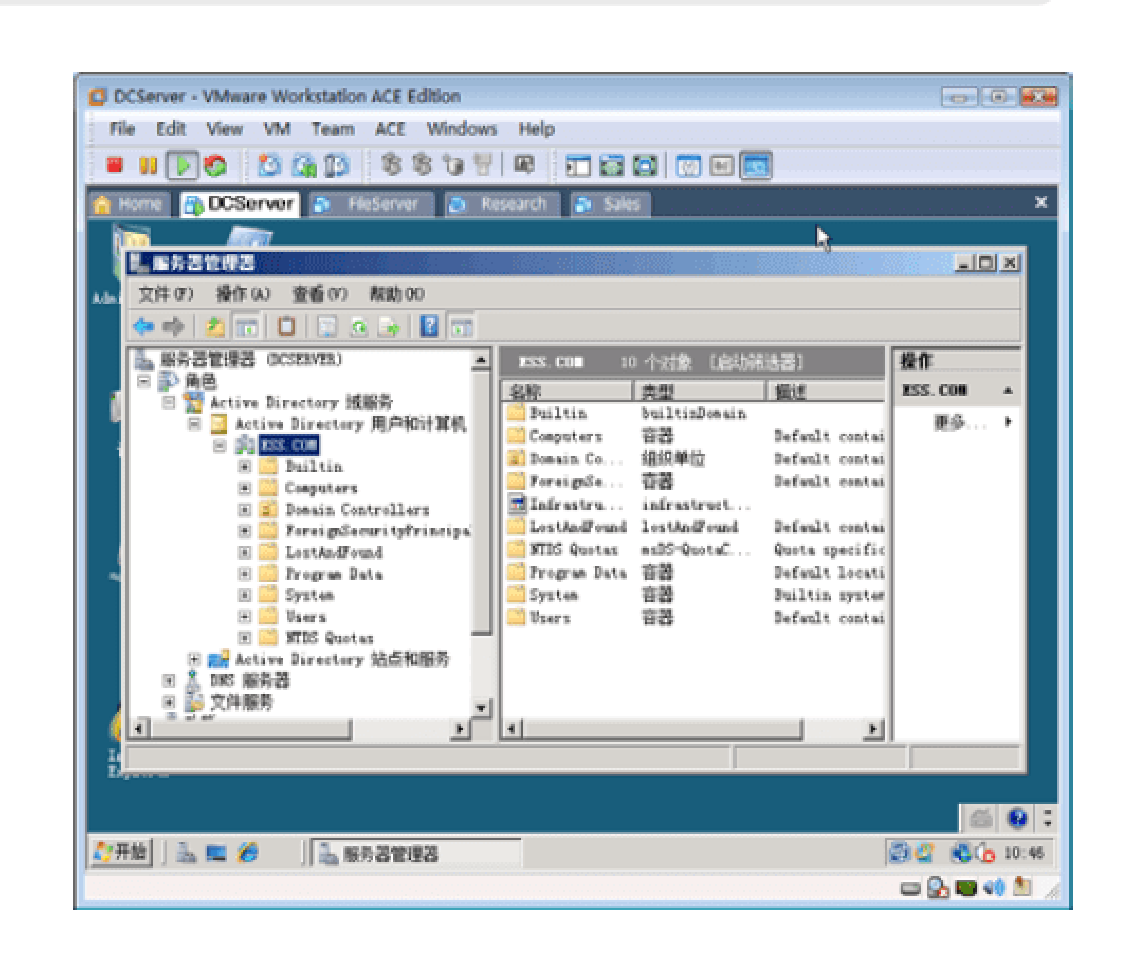


图 5-18　启用高级功能后看到的内容

5.2.3　让域控制器向 DNS 服务器注册 SRV 记录

由于某种原因，装完活动目录后发现 DNS 上的正向区域和 SRV 记录没有或不全，需要采取以下措施，强制让域控制器向 DNS 注册 SRV 记录。

下面先删除 DNS 服务器上的正向区域，同时也就删除了该区域下的所有记录。然后，将会让域控制器向 DNS 服务器注册其 SRV 记录。

①　打开“服务管理器”窗口。

②　如图 5-19 所示，右击_msdcs.Ess.com 选项，在弹出的快捷菜单中选择“删除”命令。

③　在弹出的提示框中，单击“是”按钮。

④　右击 ESS.COM 选项，在弹出的快捷菜单中选择“删除”命令。

⑤　在弹出的提示框中，单击“是”按钮。



提示：现在相当于 DNS 没有配置成功，没有正向查找区域，也没有 SRV 记录。这种情况域中的其他计算机没有办法通过 DNS 找到 ESS.COM 域的域控制器。

⑥　如图 5-20 所示，右击“正向查找区域”选项，在弹出的快捷菜单中选择“新建区域”命令。

⑦　在新建区域向导中，单击“下一步”按钮。

⑧　如图 5-21 所示，区域类型选择“主要区域”，选中“在 Active Directory 中存储区域”复选框，单击“下一步”按钮。



提示：选中“在 Active Directory 中存储区域”复选框，该区域就支持安全更新，即域中的计算机 IP 地址变化后可以向该区域注册自己的 IP 地址。

⑨ 如图 5-22 所示，在“Active Directory 区域传送作用域”界面中，选择“至此域中的所有 DNS 服务器”单选按钮。

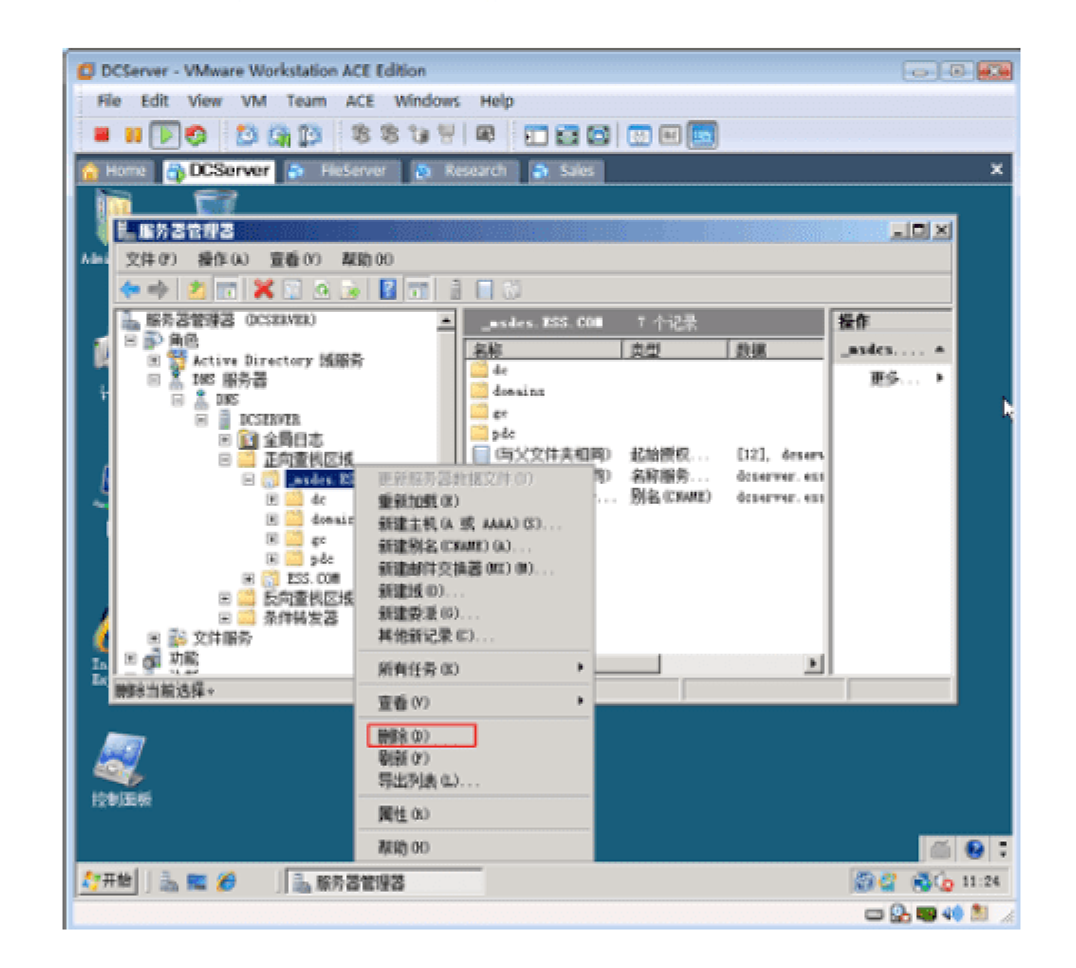


图 5-19 删除整个区域

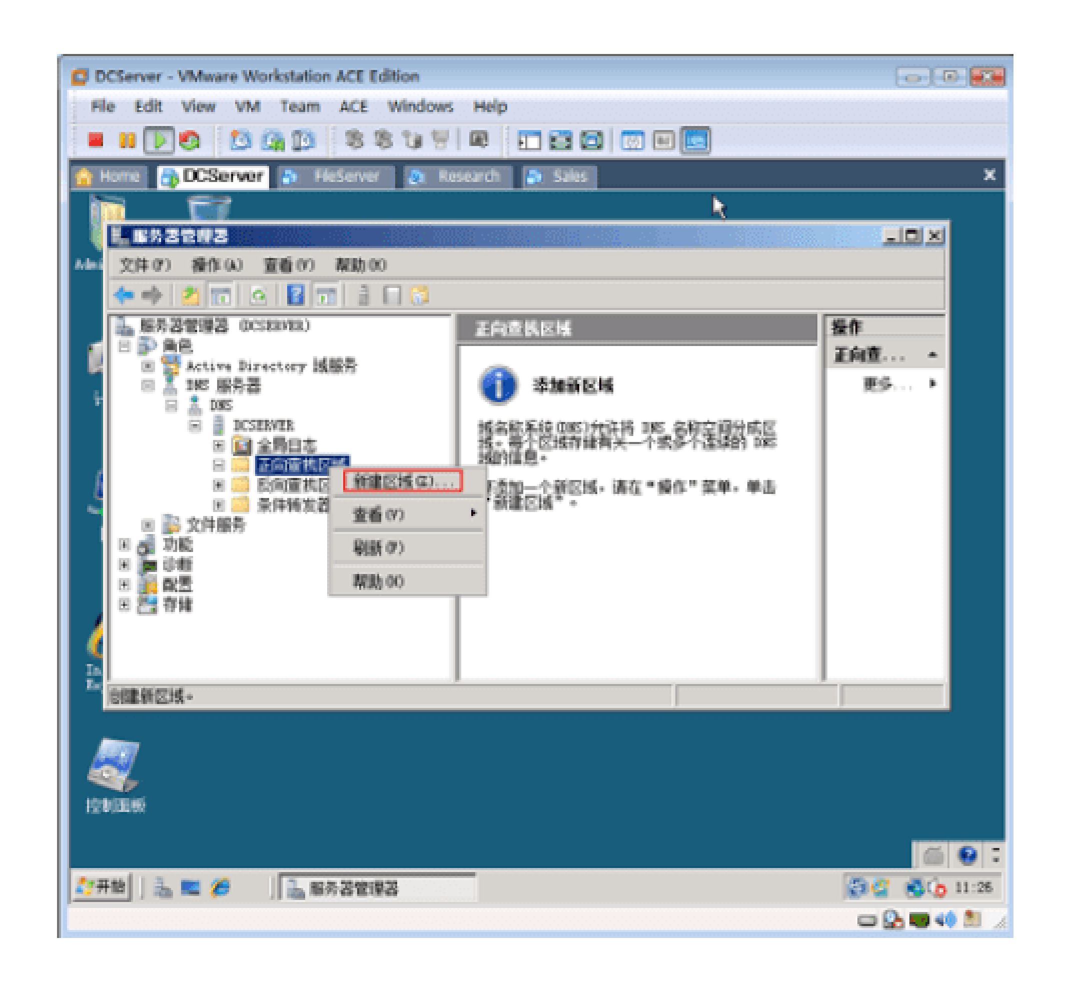


图 5-20 新建正向查找区域

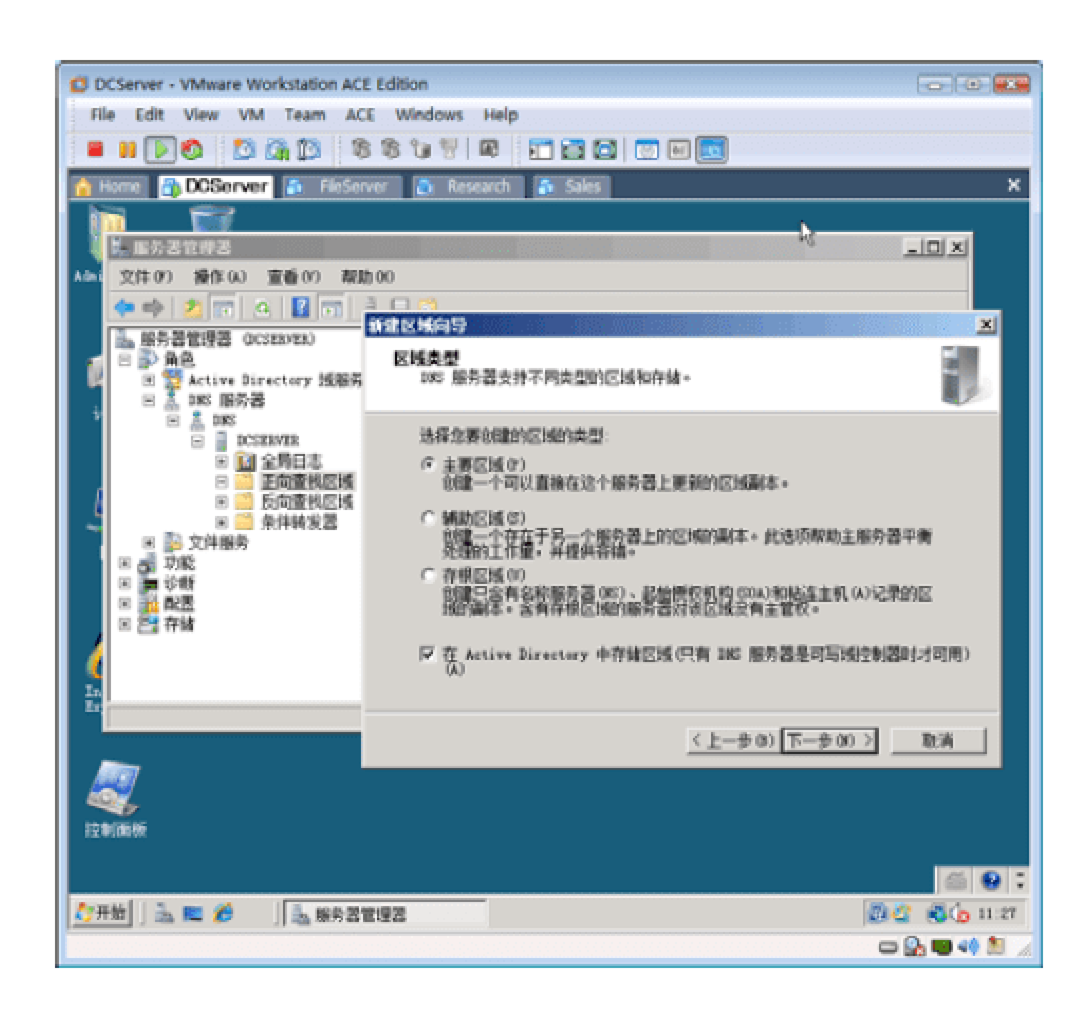


图 5-21 指定区域类型

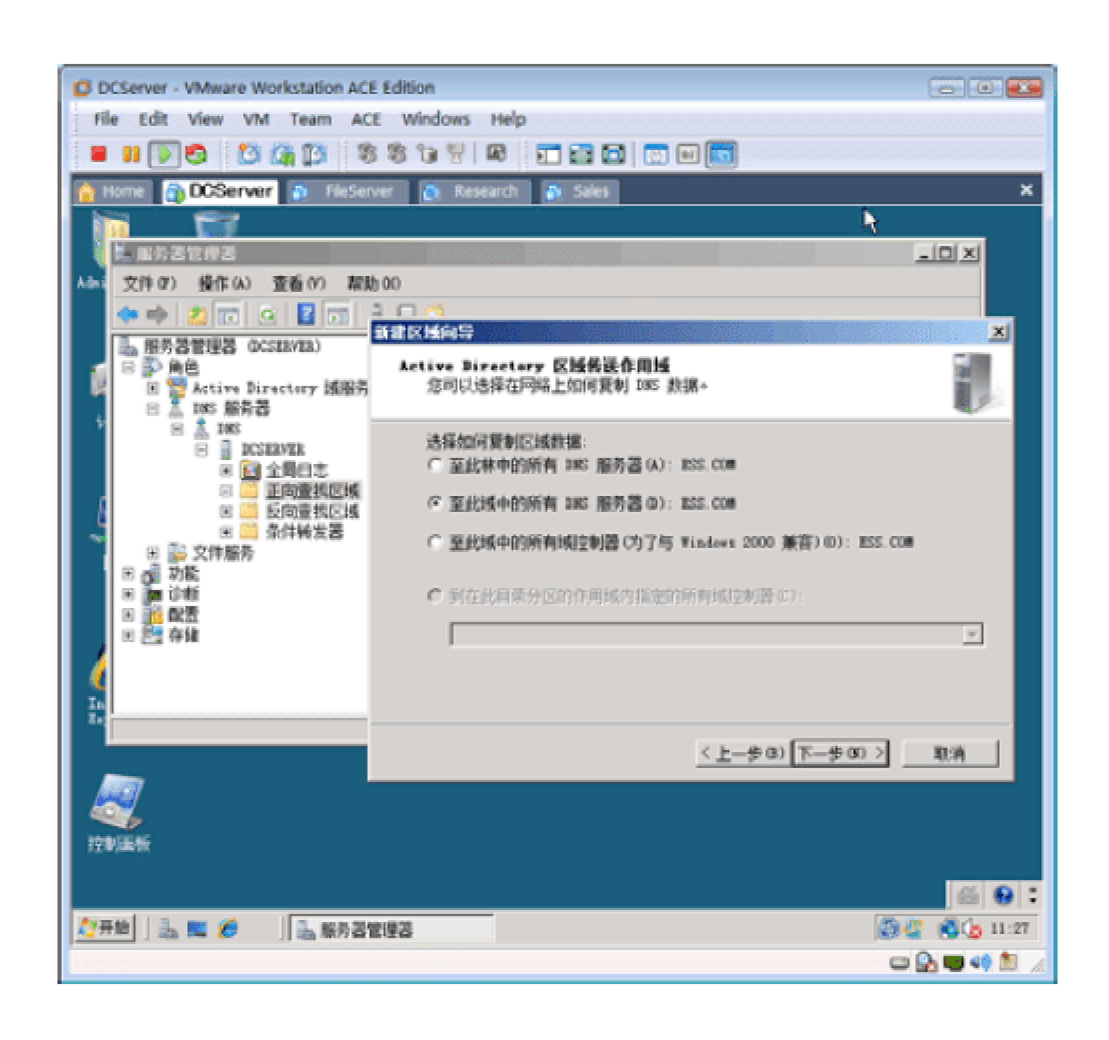


图 5-22 指定活动目录传送作用域

⑩ 如图 5-23 所示，输入区域名字_msdcs.ESS.COM，单击“下一步”按钮。


提示：_msdcs 是固定格式，比如您安装的林的名称是 sohu.com，那么需要创建一个_msdcs.sohu.com 正向查找区域。

⑪ 如图 5-24 所示，在“动态更新”界面中，选中“只允许安全的动态更新”单选按钮。
⑫ 单击“下一步”按钮，然后单击“完成”按钮。
⑬ 如图 5-25 所示，按照上面的步骤创建一个 ESS.COM 区域。这个名字必须是活动目录的名字。
⑭ 如图 5-26 所示，注意观察，刚建的两个区域下面没有 SRV 记录。
⑮ 确保域控制器的 TCP/IPv4 的首选 DNS 指向自己的地址。

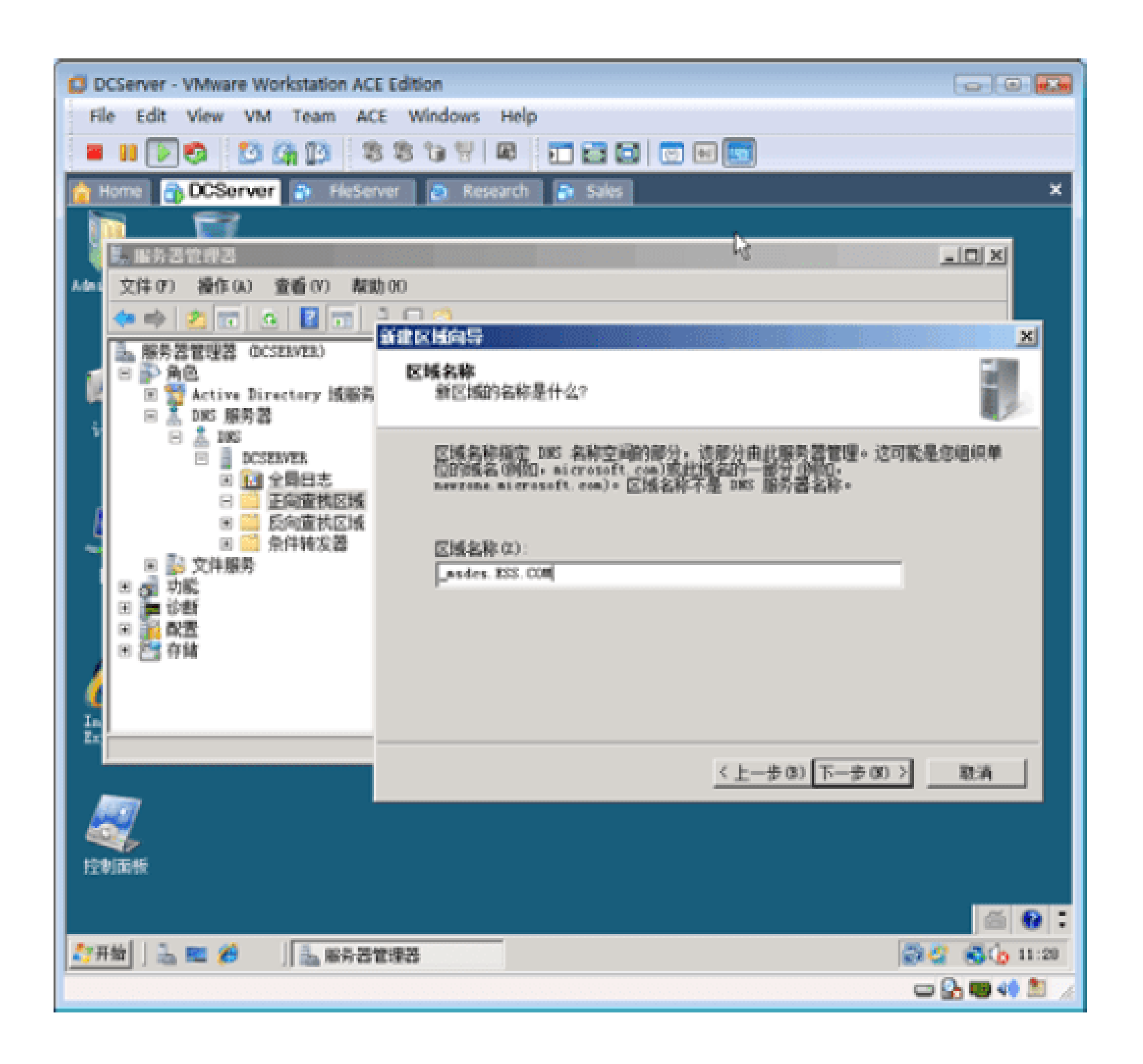


图 5-23　创建正向查找区

图 5-24　允许安全更新

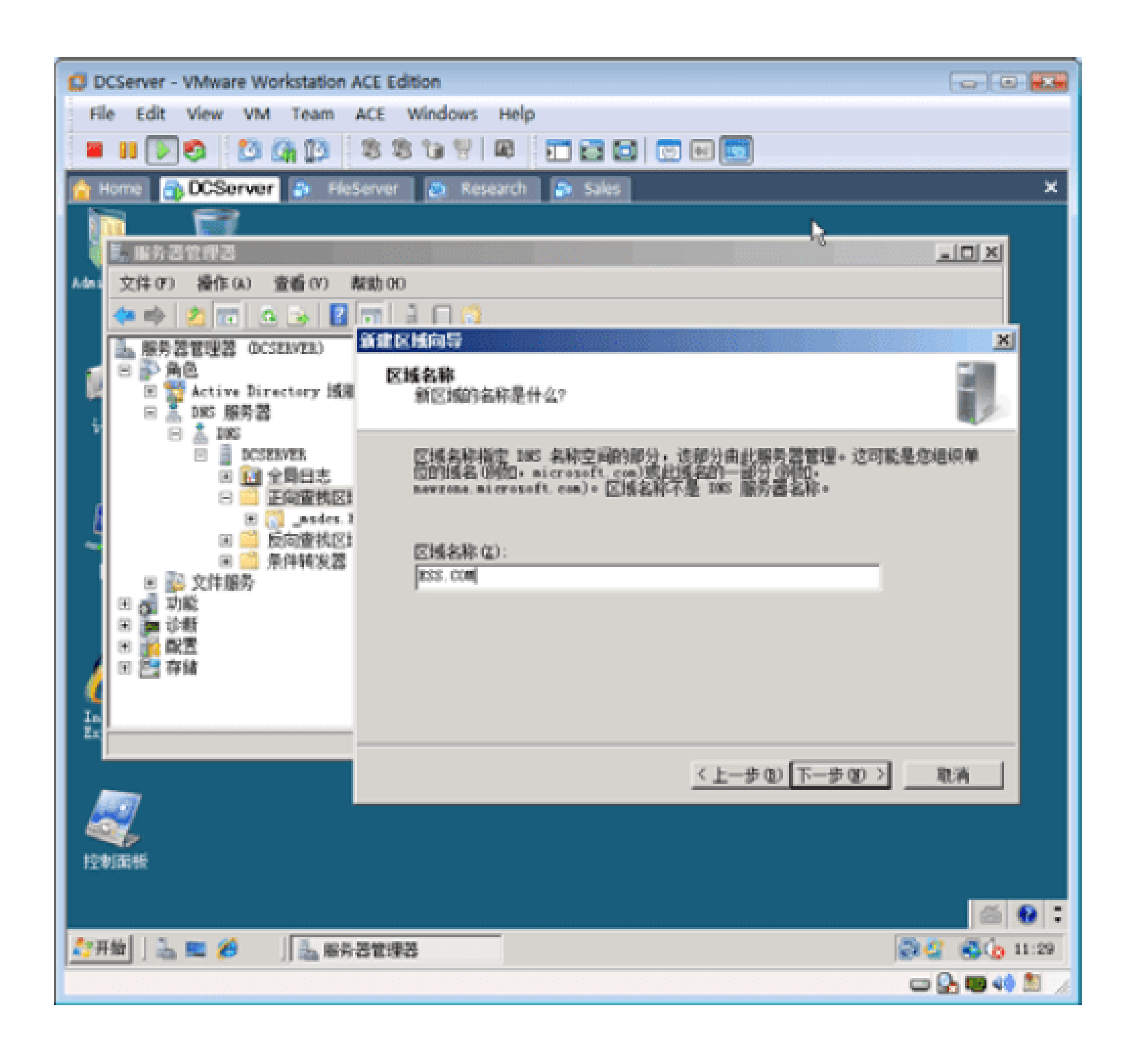
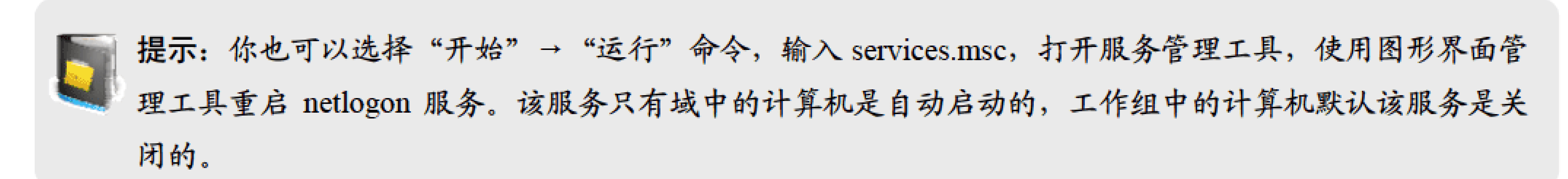


图 5-25　创建正向查找区域

图 5-26　创建好的两个正向查找区域

⑯　如图 5-27 所示，在域控制器上运行 net stop netlogon。

⑰　再运行 net start netlogon。



提示：你也可以选择“开始”→“运行”命令，输入 services.msc，打开服务管理工具，使用图形界面管理工具重启 netlogon 服务。该服务只有域中的计算机是自动启动的，工作组中的计算机默认该服务是关闭的。

⑱　选中 DNS 服务器刚才创建的两个区域，按 F5 键刷新。如图 5-28 所示，你会发现已经注册成功 SRV 记录。

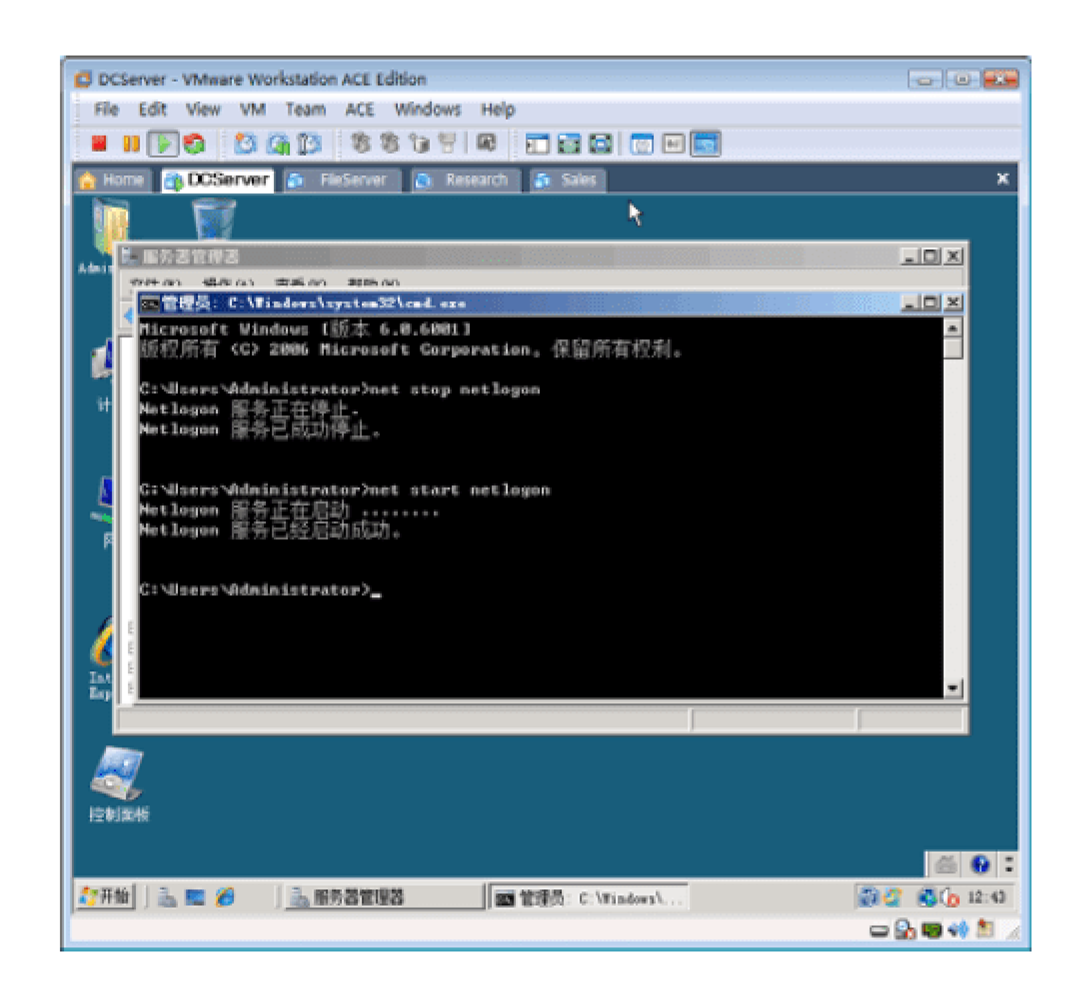


图 5-27　重启 netlogon 服务

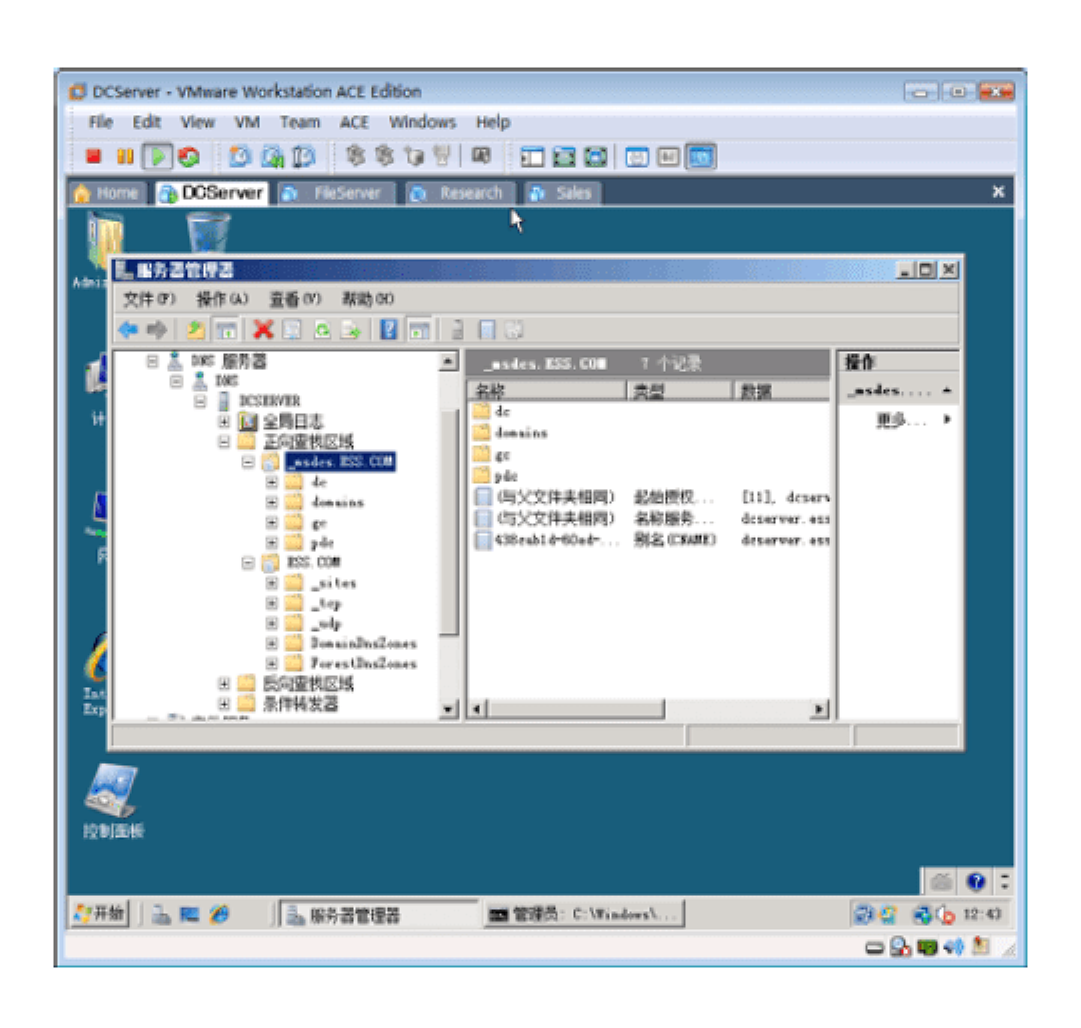


图 5-28　域控制器向 DNS 注册 SRV 记录成功

5.2.4　SRV 记录注册不成功的可能原因

默认情况，安装完活动目录 DNS 中的 SRV 记录就注册成功了，如果在域控制器上重启 netlogon 服务，有可能还是不能注册 SRV 记录到 DNS 服务器上，以下是总结的需要检查的几点。

- DNS 区域名字是否正确，是否允许安全更新。

  创建的正向查找区域的名字必须是活动目录的名字，还必须创建一个_msdcs.活动目录名字区域。双击创建的区域，如图 5-29 所示，确保动态更新是“安全”或“非安全”，不能选择“无”。

- 确保域控制器全名已经包括了活动目录的名字，如图 5-30 所示，默认是包括的。

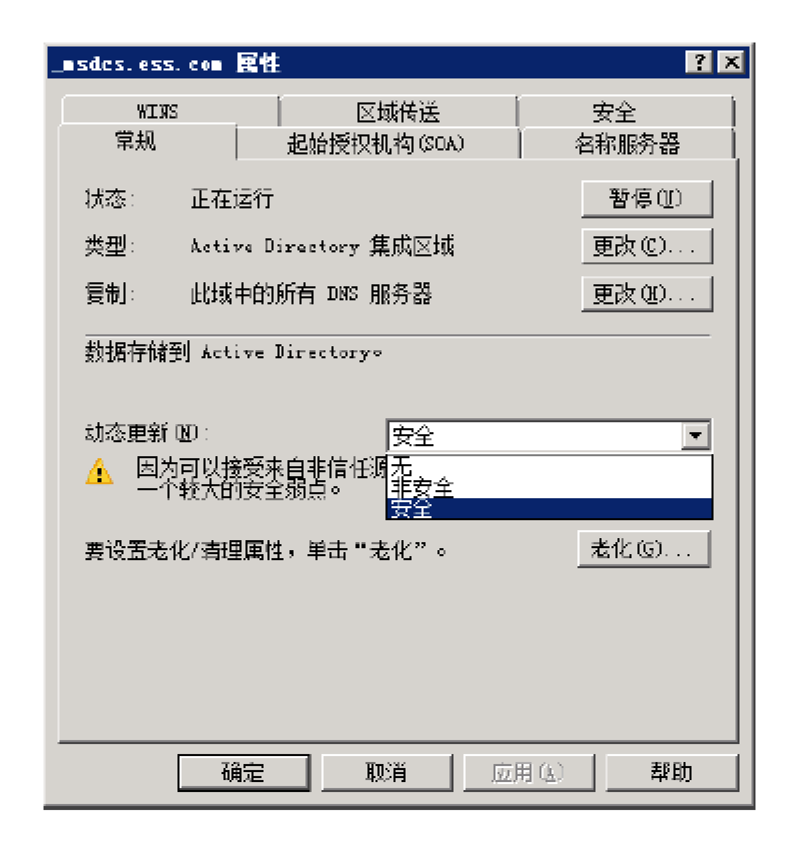


图 5-29　正向查找区允许安全更新

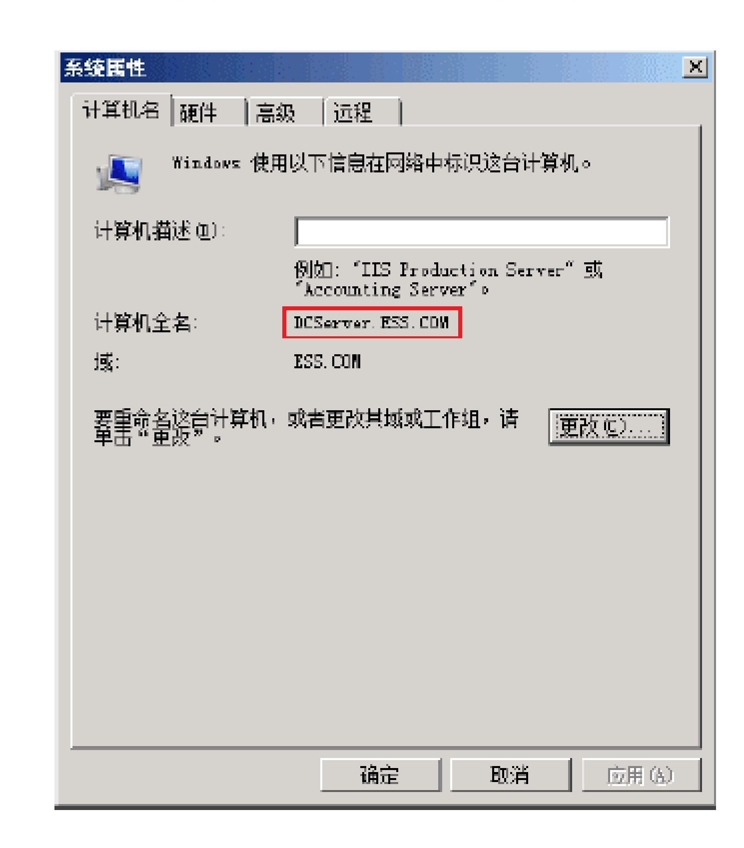


图 5-30　域控制器的全名必须有域名后缀

如果域控制器的全名没有包括 ESS.COM 后缀，单击“更改”按钮。如图 5-31 所示，在弹出的对话框中，单击“确定”按钮。

如图 5-32 所示，在“计算机名/域更改”对话框中，单击“其他”按钮。

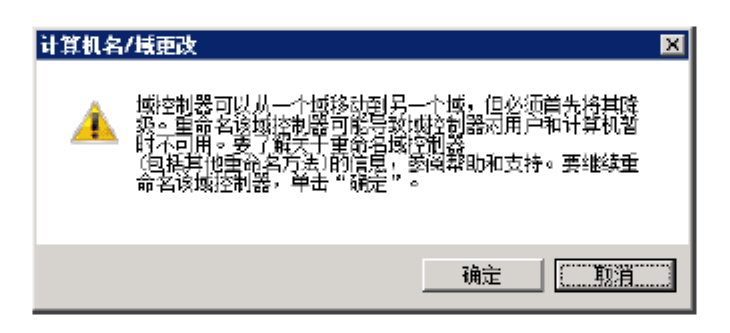


图 5-31　提示对话框



图 5-32　更改后缀

默认已经选中了“在域成员身份变化时，更改主 DNS 后缀”复选框，如图 5-33 所示，输入 ESS.COM 后缀，单击“确定”按钮。这样就给域控制器的计算机添加了一个域后缀。

- 如图 5-34 所示，确保域控制器的 TCP/IP 属性中已经选中“在 DNS 中注册此连接的地址”复选框。

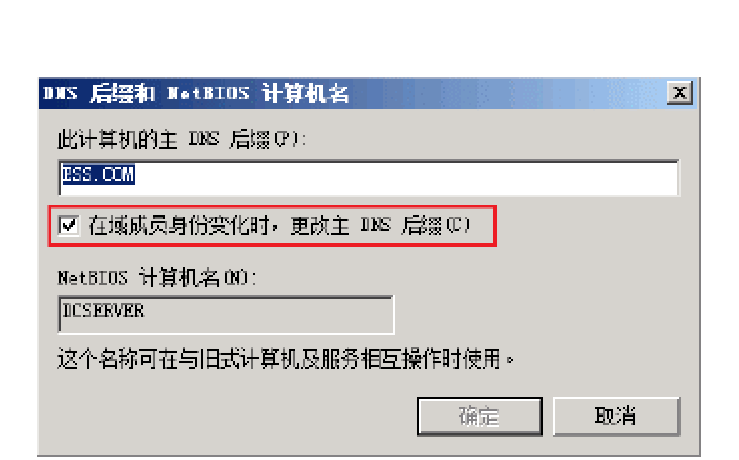


图 5-33　添加后缀

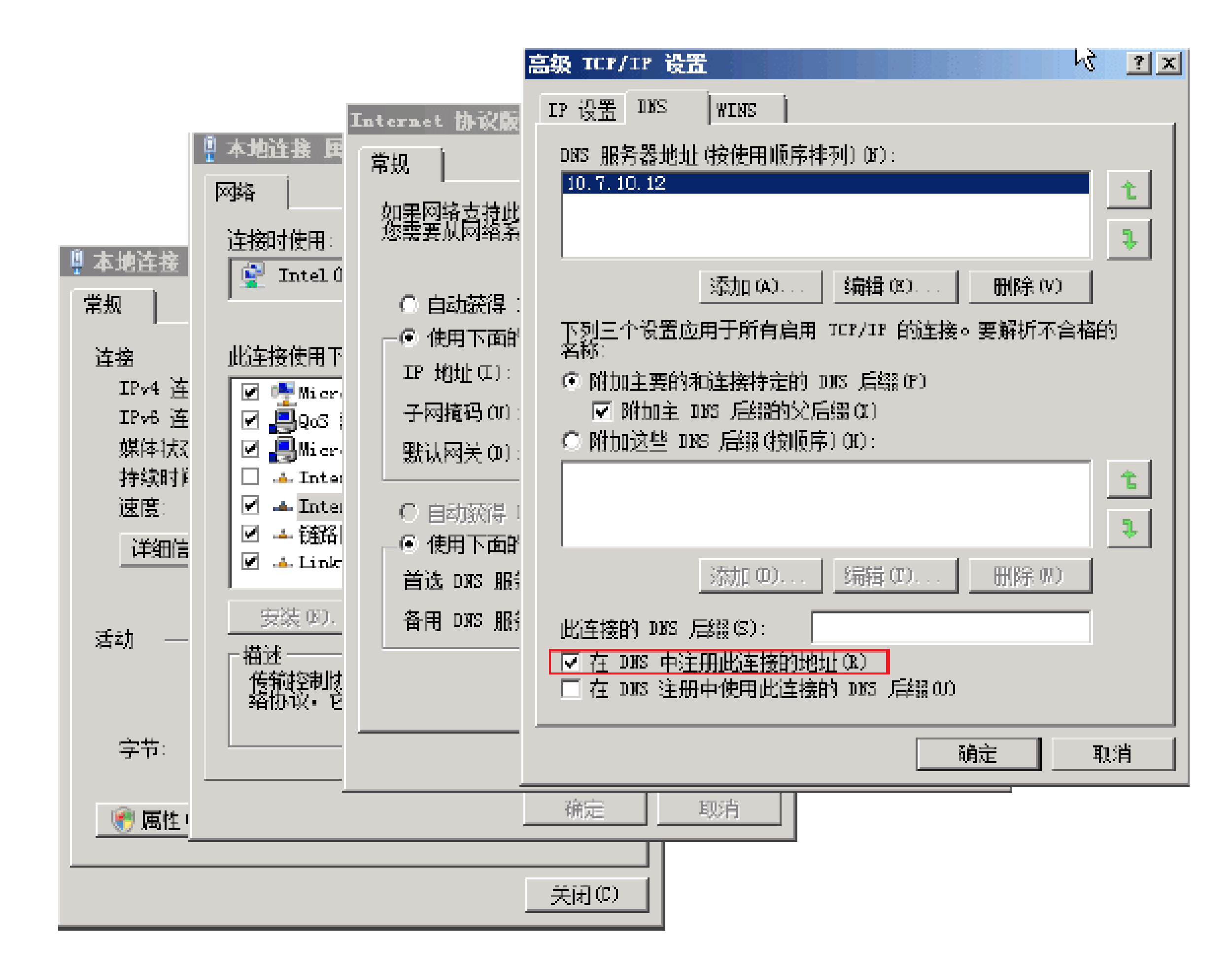


图 5-34　在 DNS 中注册此连接的地址

5.2.5　将计算机加入域

将计算机加入域可以执行以下操作。

① 将 Sales 计算机的计算机名称改为 Sales，重启系统。

② 以管理员的身份登录 Sales，更改 Sales 计算机的本地连接的首选 DNS 服务器为 10.7.10.12，如图 5-35 所示。

提示：客户机使用 DNS 定位域控制器，因此必须使用内网的 DNS 服务器，不能使用 Internet 上的 DNS 服务器，如果是笔记本电脑，有可能在家或出差时使用，备用的 DNS 可以使用 Internet 上的 DNS 服务器。

③ 如图 5-36 所示，右击“计算机”图标，在弹出的快捷菜单中选择“属性”命令。

④ 在出现的“系统”对话框中，单击“改变设置”按钮。

⑤ 在出现的“系统属性”对话框中，单击“更改”按钮，如图 5-37 所示。

⑥ 如图 5-38 所示，在出现的“计算机名/域更改”对话框中，输入 ESS.COM 域名，单击“确定”按钮。

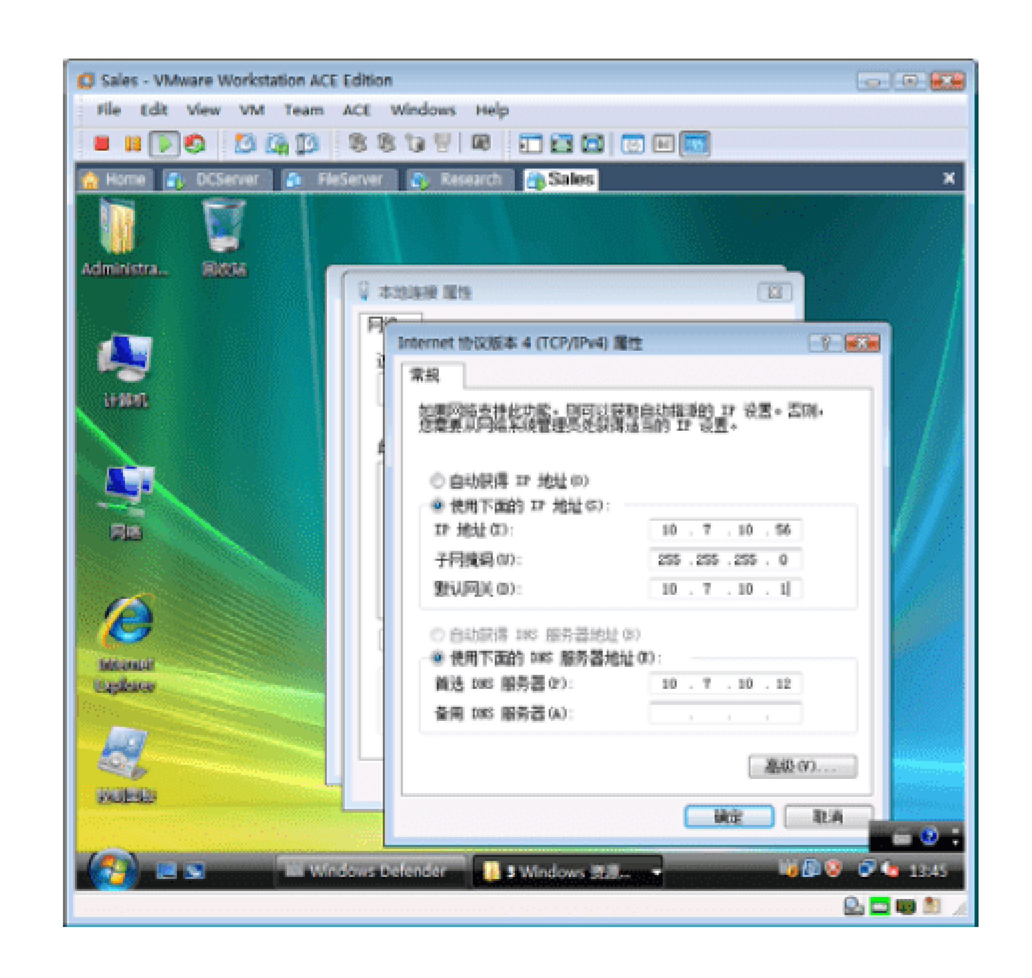


图 5-35　更改本地连接的首选 DNS

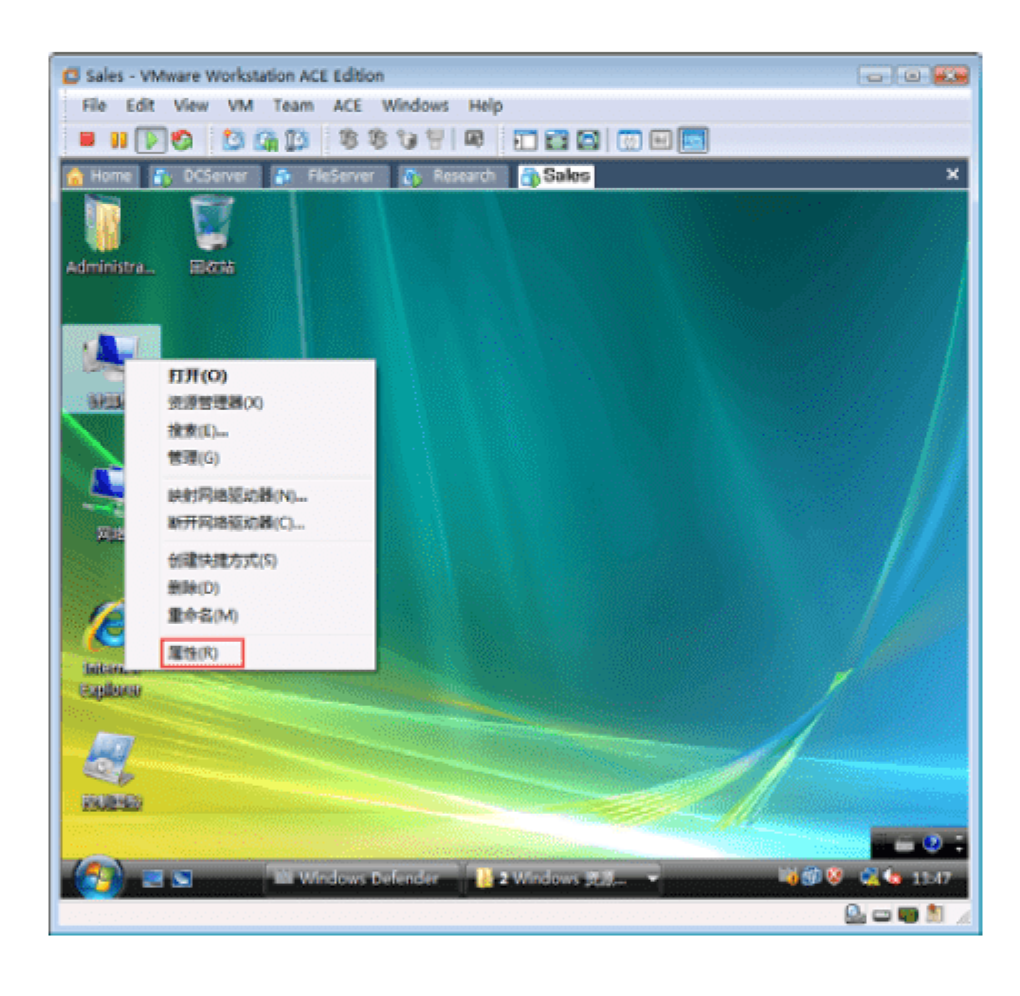


图 5-36　打开系统属性

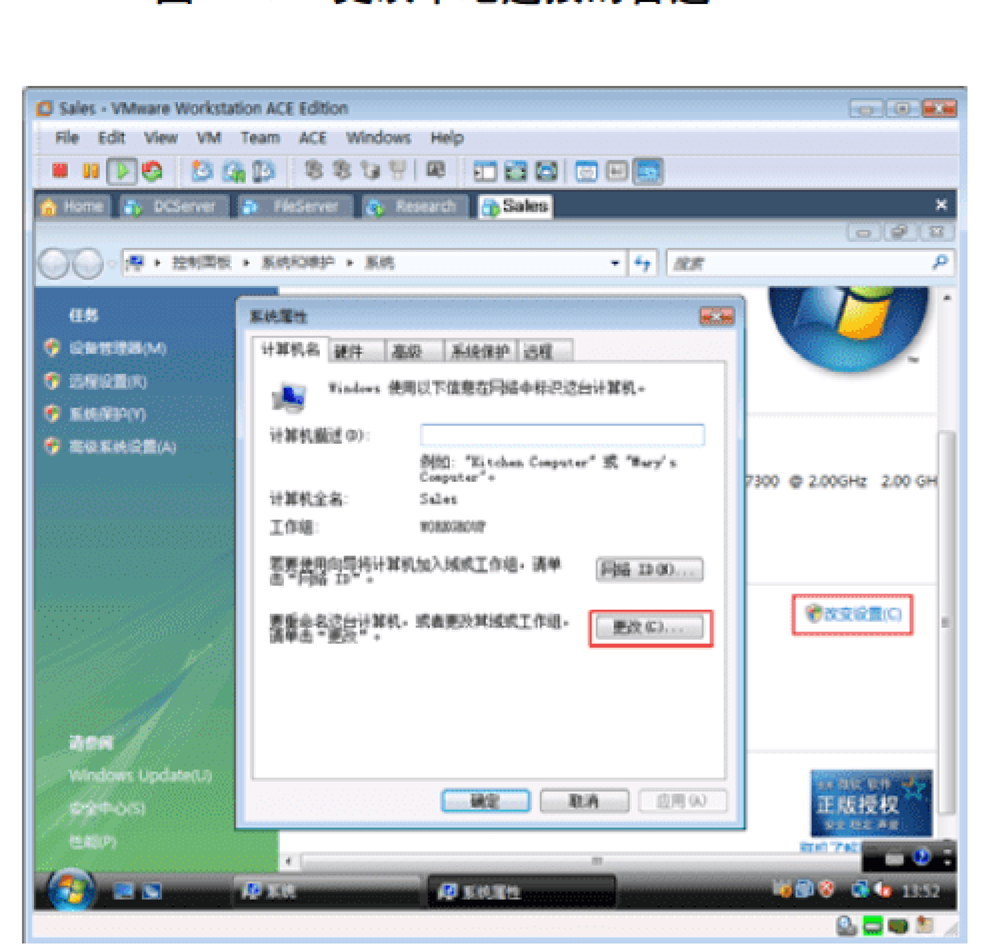


图 5-37　更改系统属性

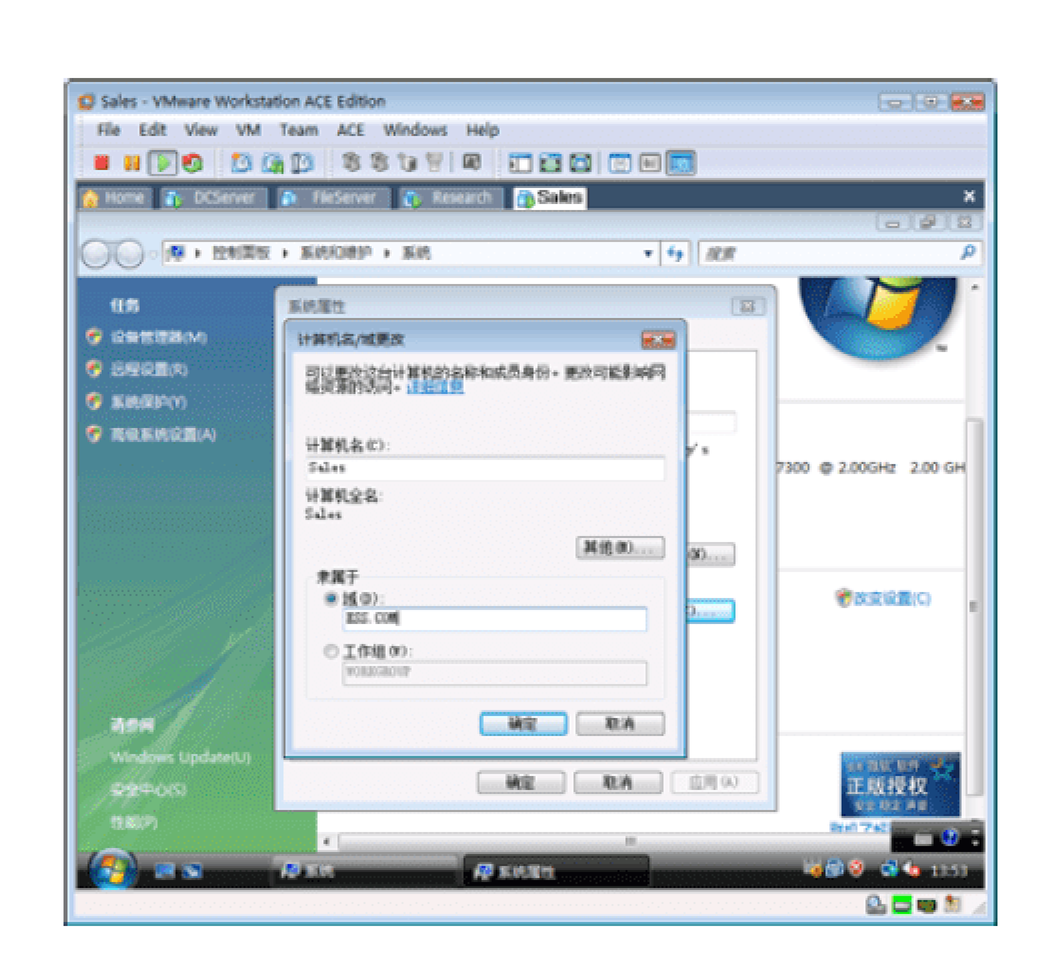


图 5-38　将计算机加入到域

⑦ 如图 5-39 所示，在出现的 Windows 安全对话框中，输入域管理员账户和密码，单击“确定”按钮。



提示：域中的非管理员用户也可将计算机加入到域。

⑧ 如图 5-40 所示，提示成功加入域，重启计算机。



注意：将计算机加入域后，将自动在活动目录的 computers 目录下创建计算机账户。另外，还可以在活动目录中先创建计算机账户，再将计算机加入域，这样实体计算机和计算机账号将自动关联。

若将计算机脱离域，只需将计算机加入工作组即可从域中退出。



图 5-39 输入域管理员账户和密码

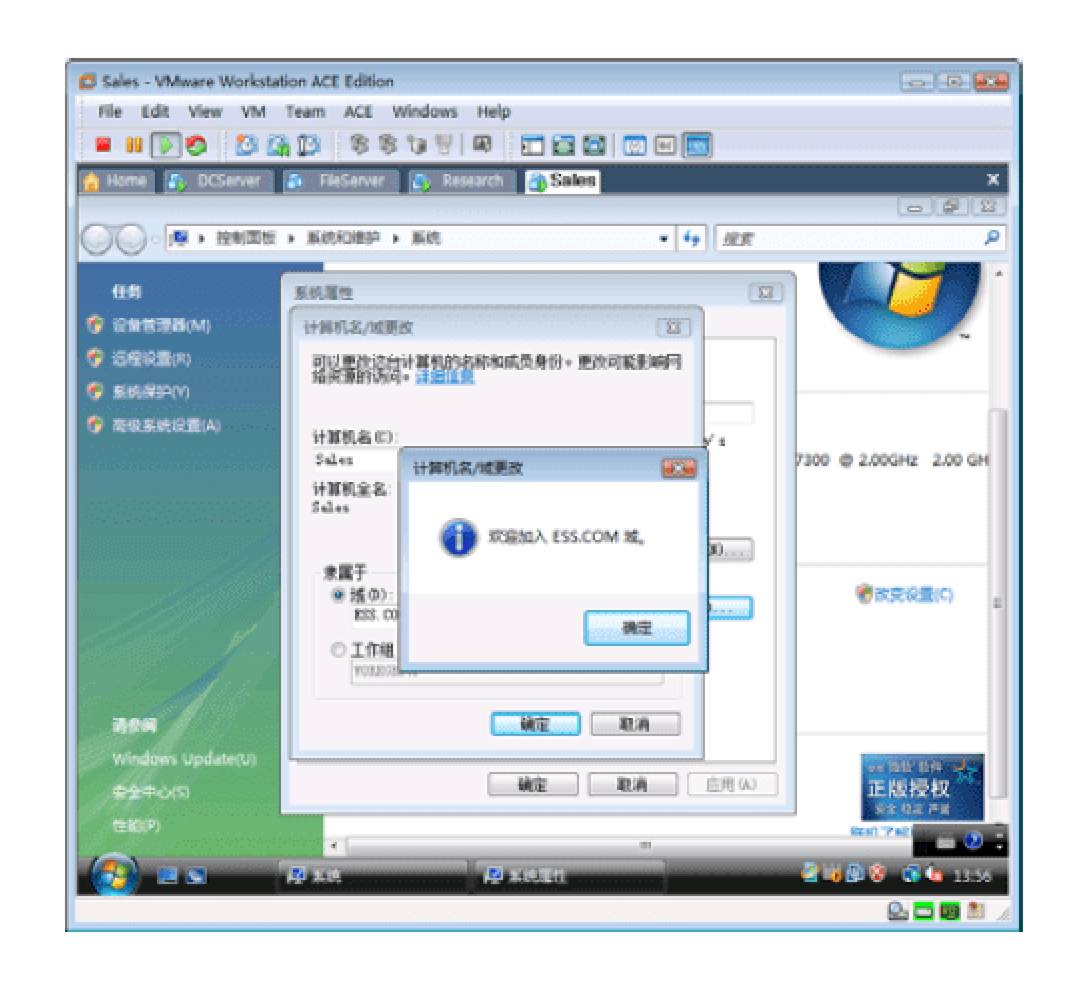


图 5-40 成功加入域

⑨ 如图 5-41 所示，检查加入到域之后计算机的名称，发现计算机名称后自动添加了域后缀。

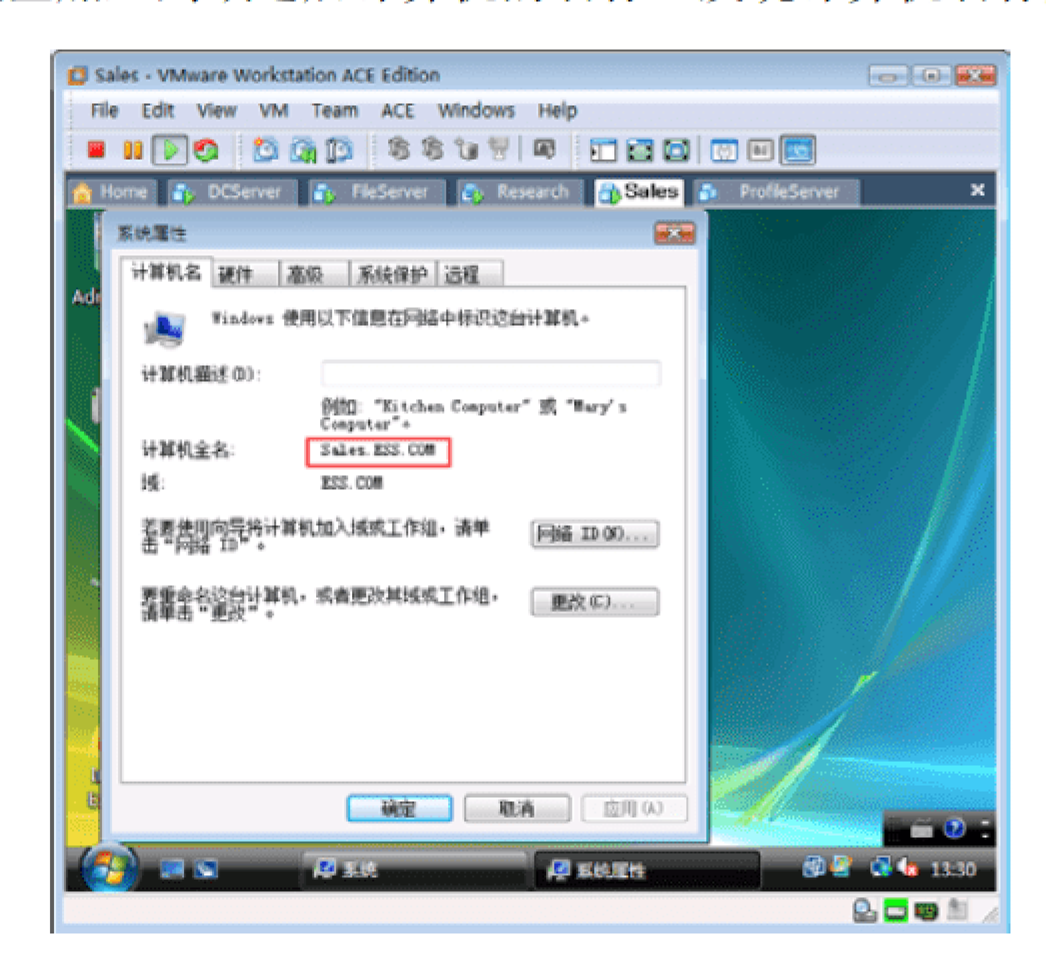


图 5-41 计算机全名

5.2.6 将 Windows Server Core 操作系统加入域或退出域

1. 任务

- 查看和更改计算机名称。
- 更改 IP 地址和 DNS。

- 将计算机加入到域。

2. 步骤

① 打开安装有 Windows Server Core 的 ProfileServer 虚拟机。
② 以管理员的身份登录 ProfileServer 虚拟机。
③ 如图 5-42 所示，输入 hostname，查看计算机名称。
④ 输入 netdom renamecomputer FileServer /newname:ProfileServer，更改计算机名称为 ProfileServer。
⑤ 如图 5-43 所示，输入 netsh interface ipv4 set address name=“本地连接” source=static addr=10.7.10.212 mask= 255.255.255.0 gateway=10.7.10.1，更改本地连接的 IP 地址、子网掩码和网关信息。

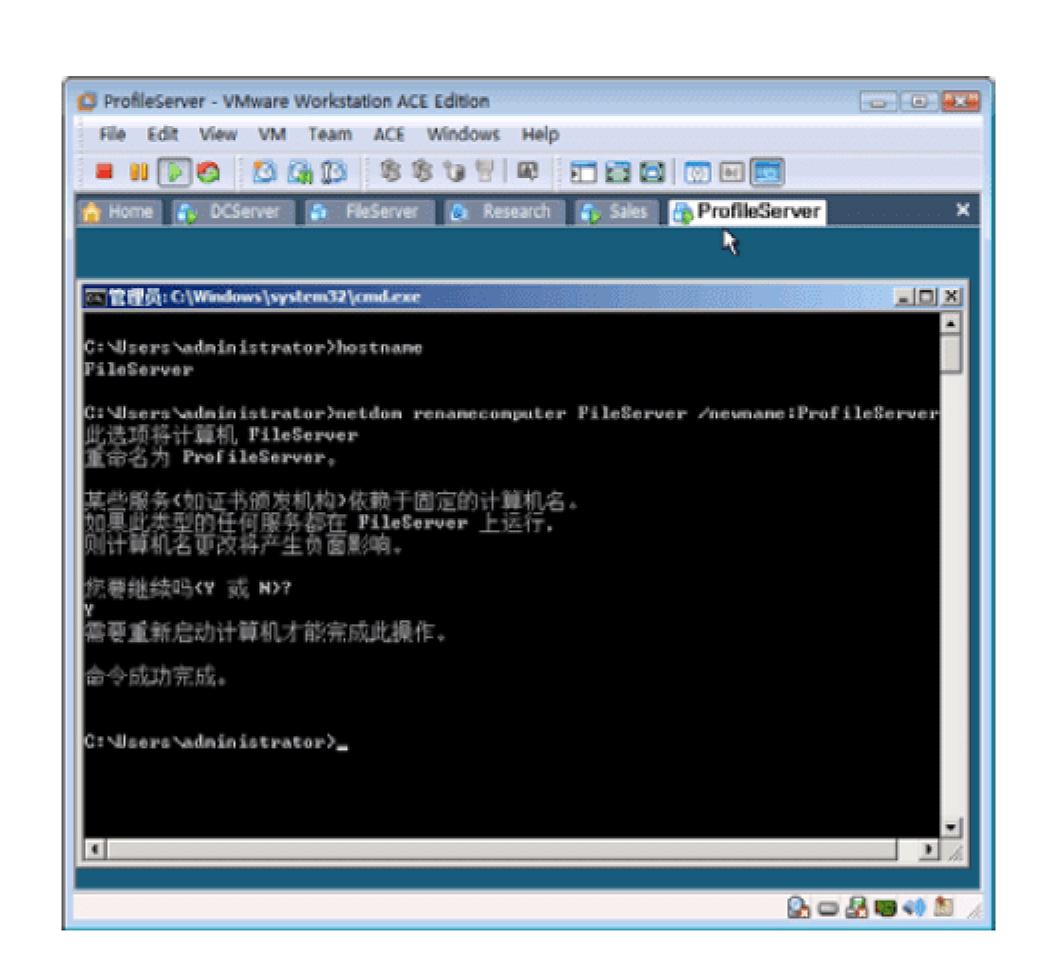


图 5-42　更改计算机名称

图 5-43　更改 IP 设置

⑥ 输入 netsh interface ipv4 set dnsserver “本地连接” static 10.7.10.12 primary。
⑦ 输入 shutdown /r /t 0，重启系统。
⑧ 以本地管理员身份登录到 ProfileServer。
⑨ 将计算机加入域，输入 netdom join %computername% /domain:Ess.com /userd:administrator /passwordD:a1! /REBoot:5。
⑩ 5s 后自动重启系统。


提示：参数 UserD，输入域用户。
参数 PasswordD，输入域用户的密码。

⑪ 计算机加入域后，计算机账户默认在 Computers 目录下，如图 5-44 所示。
⑫ 将计算机退出域，输入 netdom remove %computername% /domain:Ess.com /UserD:administrator /PasswordD:a1! /REBoot:5。
⑬ 5s 后自动重启。

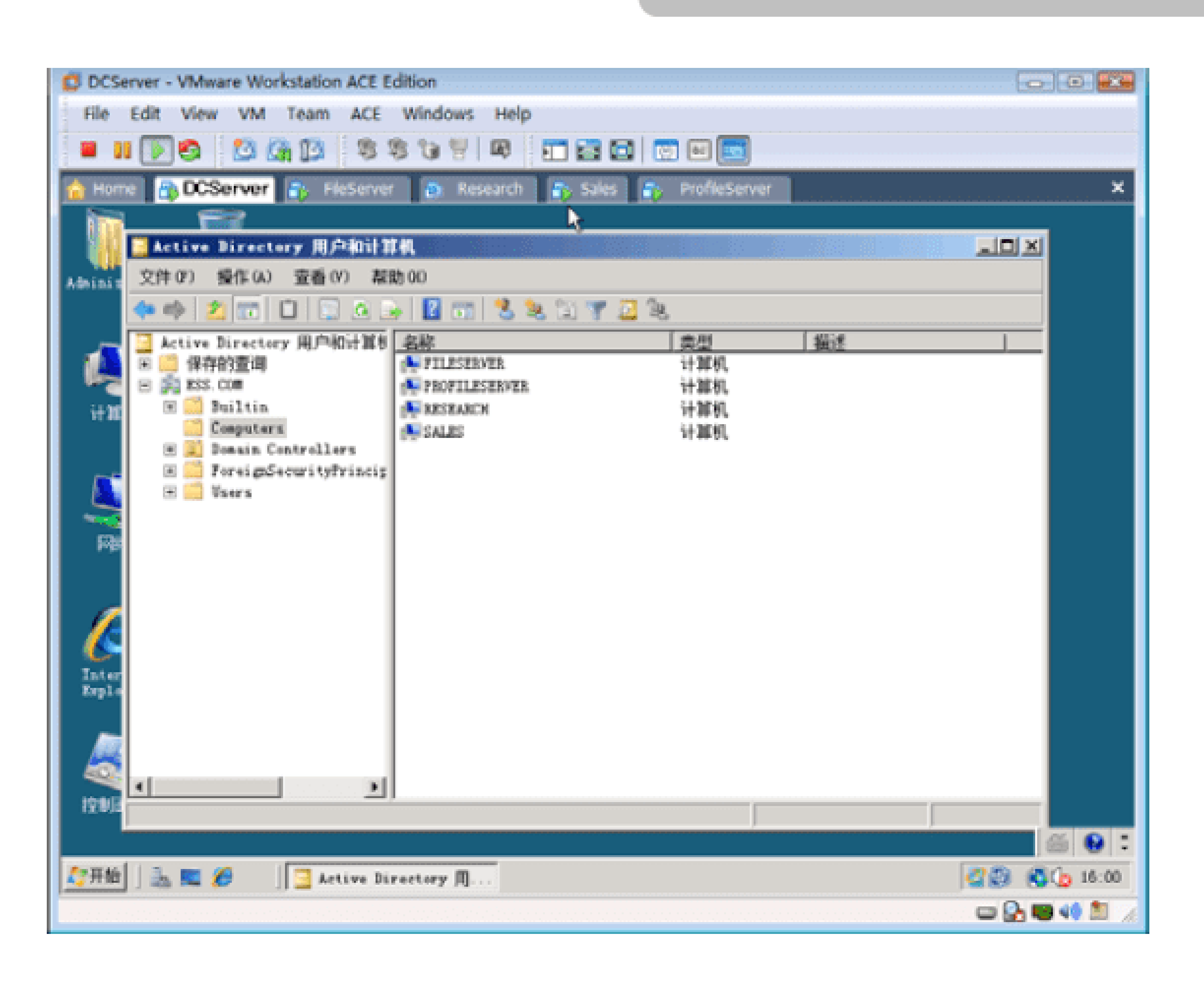


图 5-44　域中计算机账号

5.3　设计活动目录组织单位

域是活动目录逻辑结构的核心，可以在活动目录中根据管理的方便依据公司或企业的组织结构创建组织单位。

比如，管理的公司位于北京和石家庄两个城市，公司有两个部门——研发部和销售部，这两个部门分布在两个城市。若考虑 IT 部门的管理方便，可以优先以地理位置创建组织单位，再在石家庄和北京两个组织单位内按部门创建子组织单位，如图 5-45 所示。

如果公司网络和计算机管理是以部门划分的，这样就较为容易授权一个 IT 人员管理两个城市的研发部，授权一个 IT 人员管理两个城市的销售部。组织单位的创建应该以部门优先，再以地理位置创建子组织单位，如图 5-46 所示。

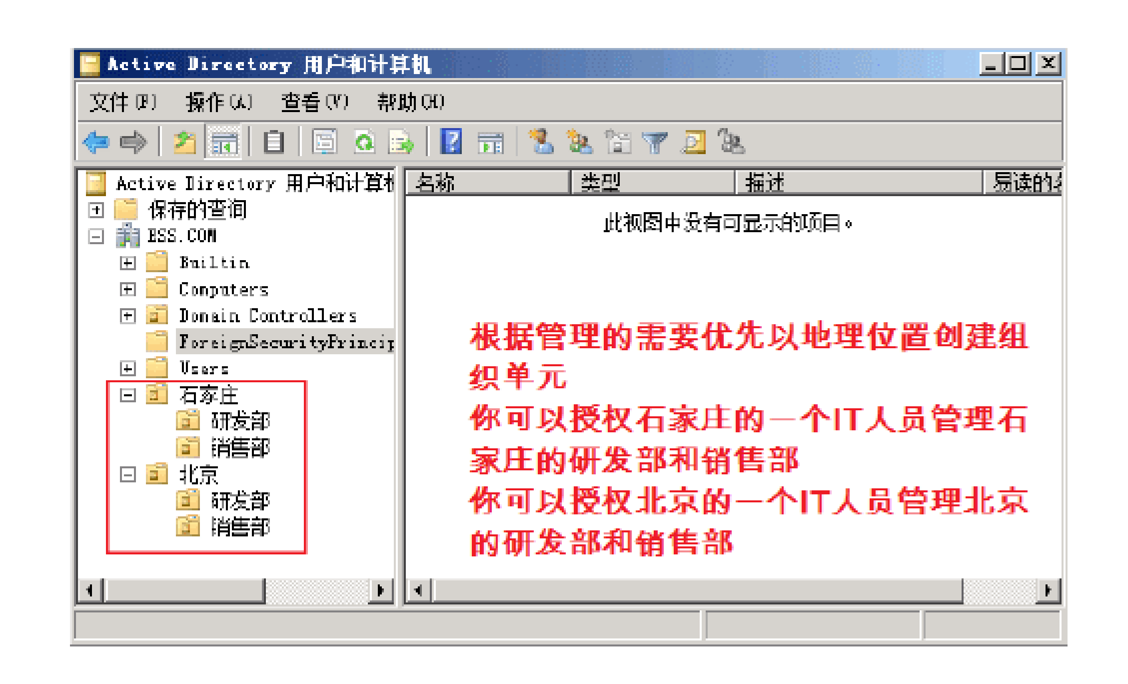


图 5-45　以地理位置创建组织单位

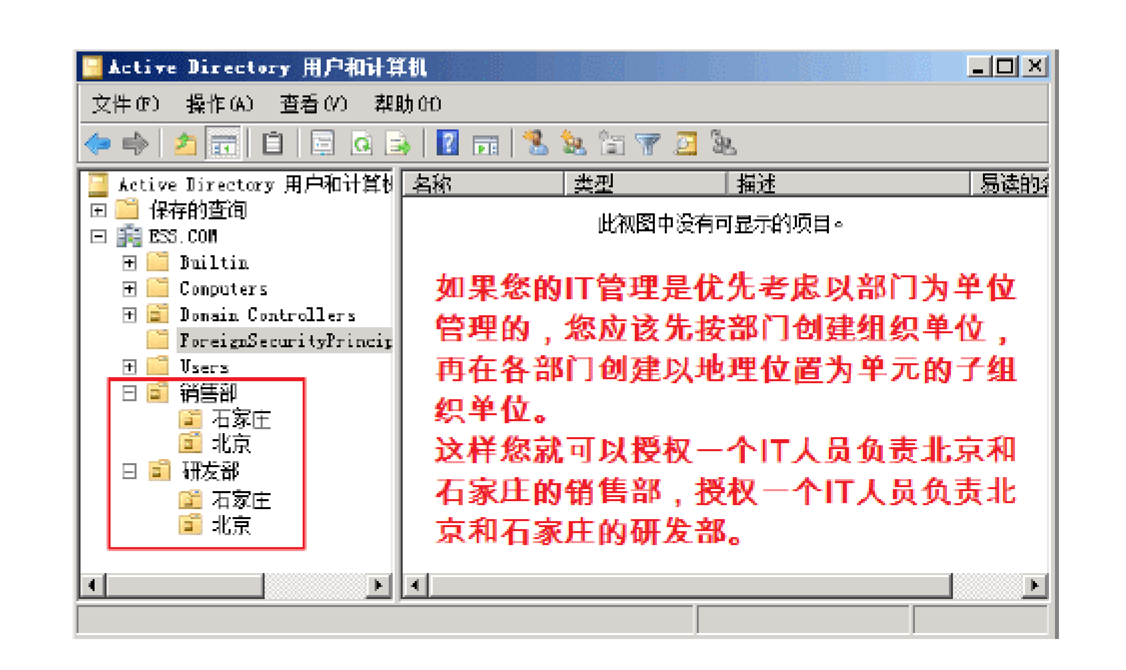


图 5-46　以部门创建组织单位

5.3.1　创建组织单位

根据公司的管理需要创建基于部门的组织单位。

① 选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开活动

目录管理工具。

② 如图 5-47 所示，右击 ESS.COM 选项，在弹出的快捷菜单中选择“新建”→“组织单位”命令。

③ 如图 5-48 所示，在出现的“新建对象-组织单位”对话框中，输入组织单位的名称，默认选中“防止容器被意外删除”复选框，单击“确定”按钮。

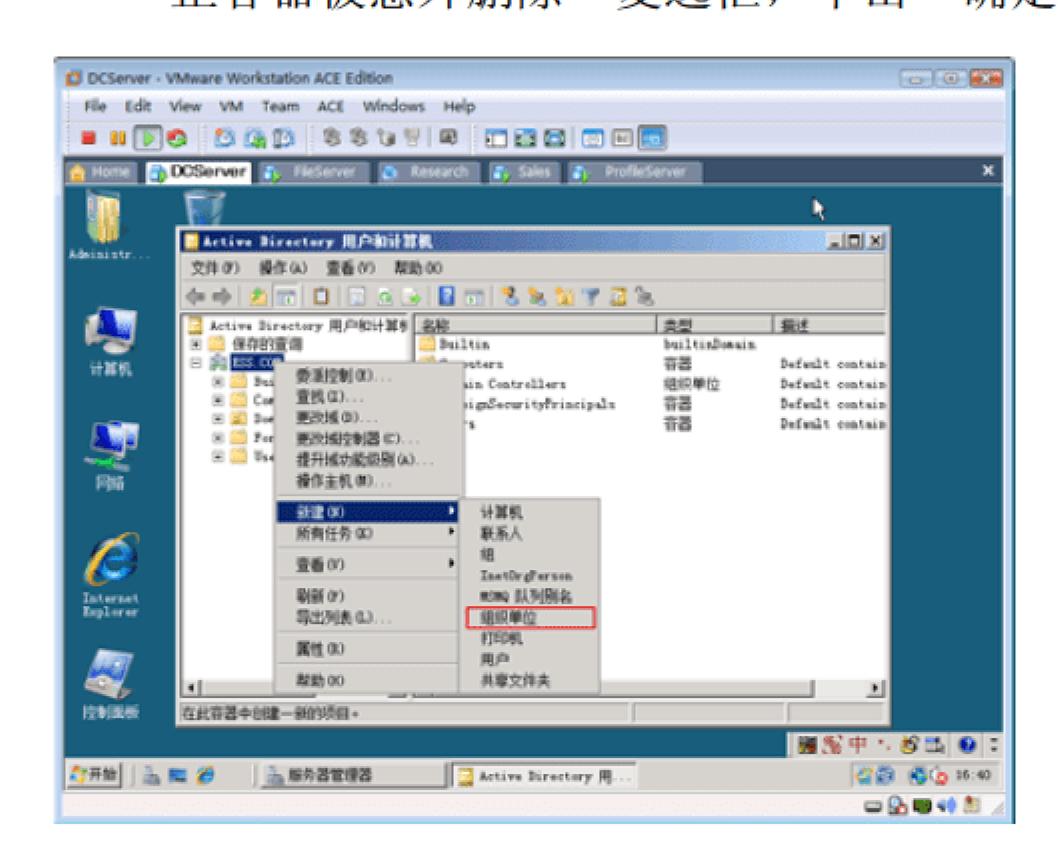


图 5-47　创建组织单位

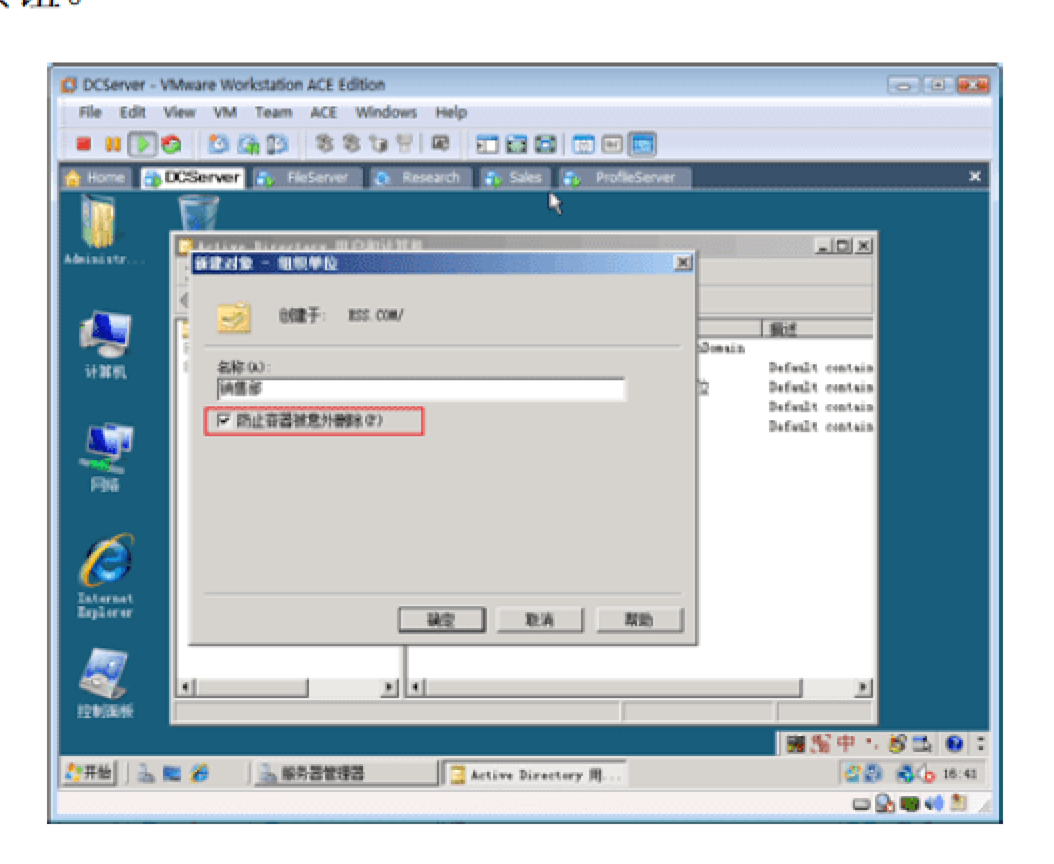


图 5-48　输入组织单位名称

④ 右击“销售部”选项，在弹出的快捷菜单中选择“新建”→“组织单位”命令，这样将会在“销售部”中创建子组织单位。为了管理起来有条理，可在各个部门创建“用户”和“计算机”组织单位。创建结果如图 5-49 所示。

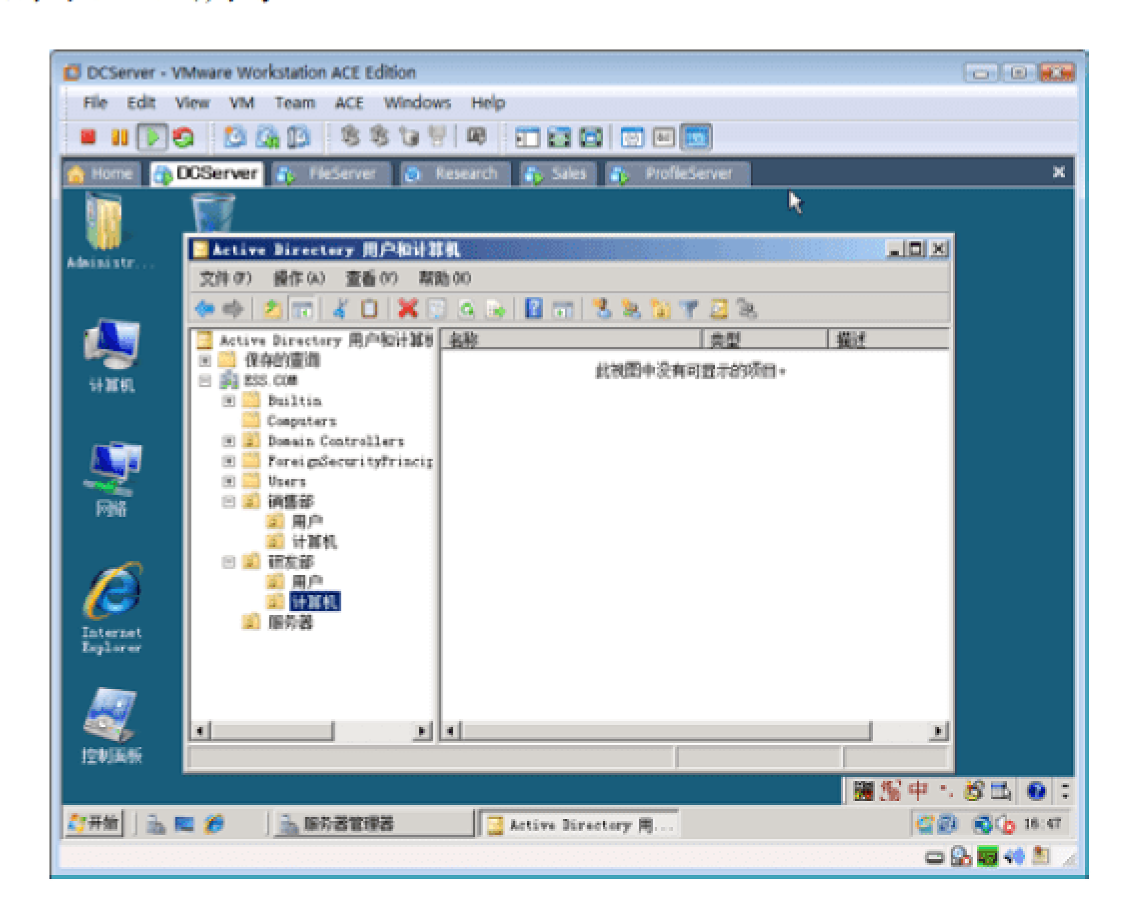


图 5-49　组织单位层次结构

5.3.2　将计算机和用户移动到组织单位

计算机加入域后，计算机账户在活动目录 computers 目录下。根据管理的需要将 FileServer 和 ProfileServer 移动到“服务器”组织单元。将 Sales 计算机账户移动到“销售部”，将 Research 移动到“研发部”。

① 选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开活动目录管理工具。

② 选中 Computers 目录下的 FileServer，按 Ctrl 键，选中 ProfileServer 计算机账户，右击选中的计算机账户，在弹出的快捷菜单中选择“移动”命令，如图 5-50 所示。

③ 如图 5-51 所示，在出现的“移动”对话框中，选中“服务器”选项，单击“确定”按钮。

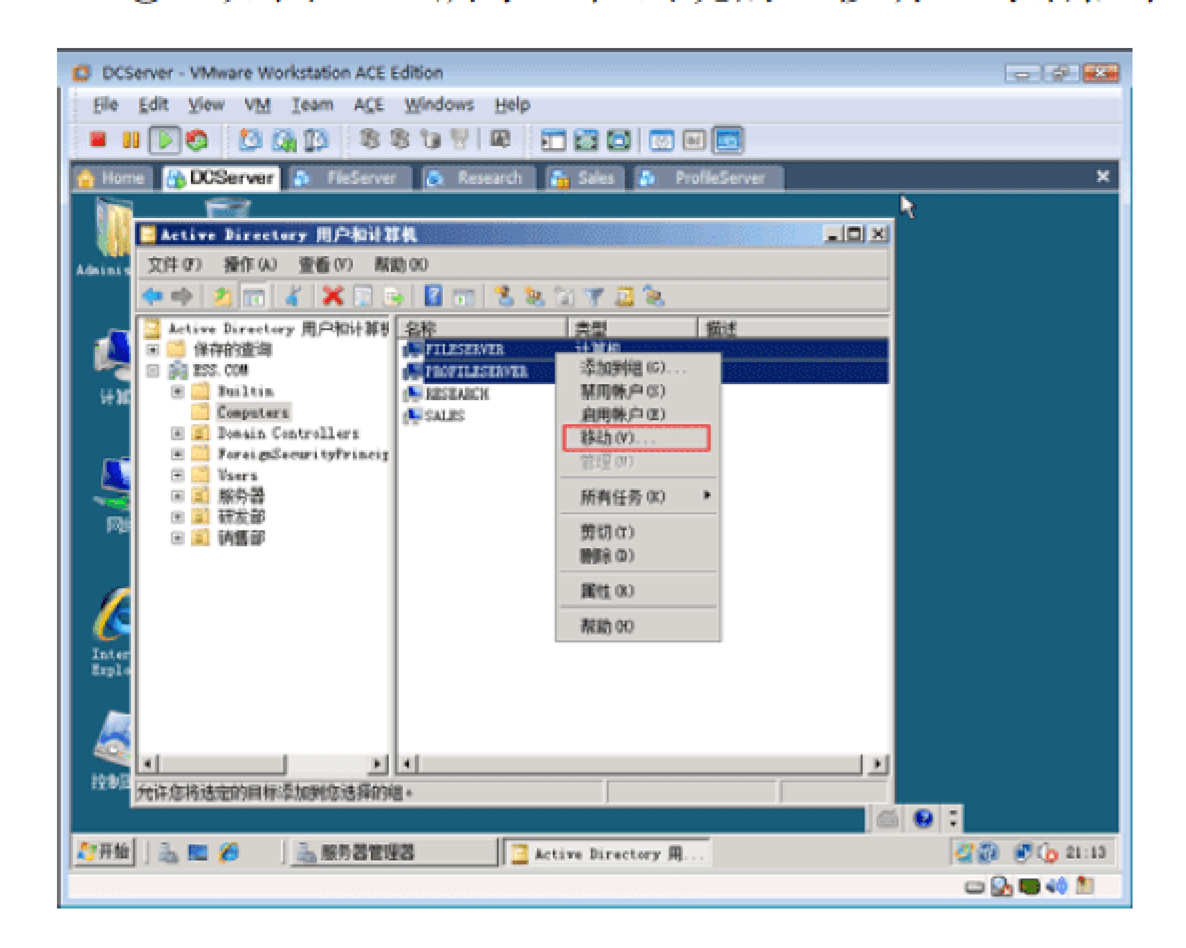


图 5-50　移动选定的计算机

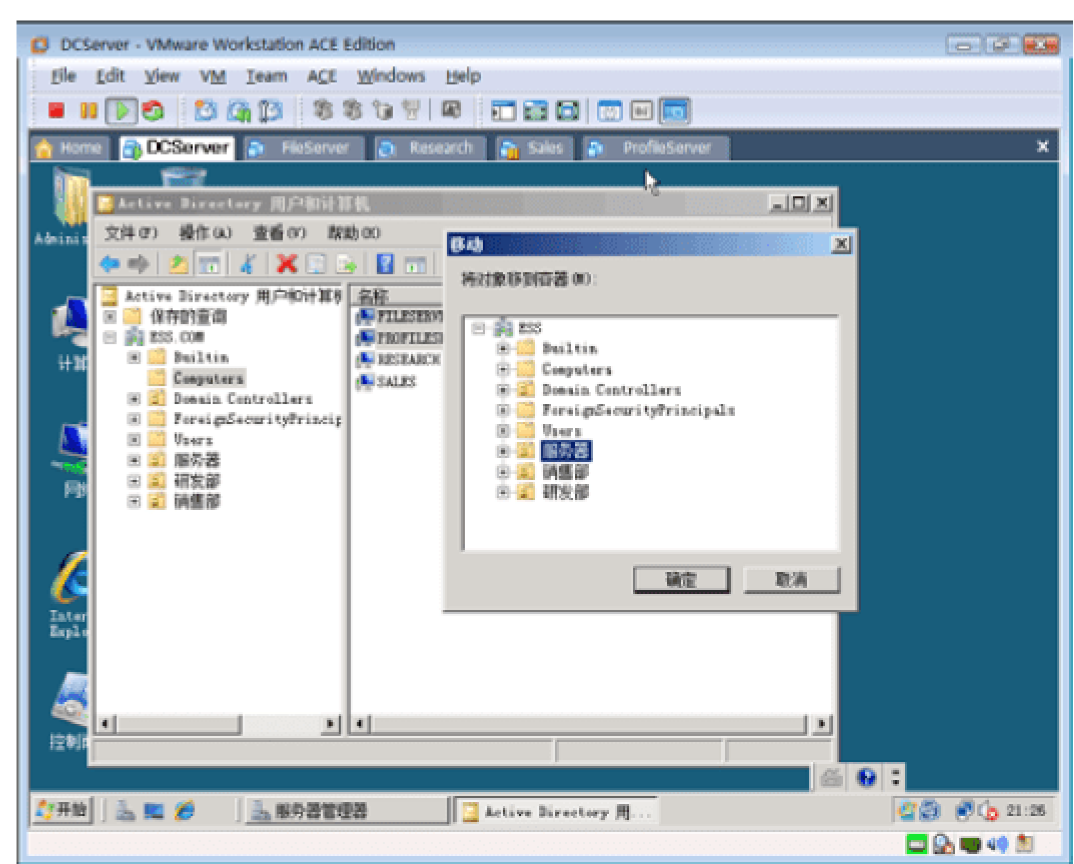


图 5-51　选择目标组织单元



提示：可直接将选中的计算机账户或用户账户拖曳到其他的组织单元。

将 Sales 计算机账户拖曳到“销售部”组织单元下的“计算机”组织单元中。将 Research 计算机账户拖曳到“研发部”组织单元下的“计算机”组织单元中。

5.4　创建和管理域用户

域用户账户是在整个域中的用户账户，存储在域控制器中的活动目录中。默认可以在加入域的计算机上登录，由域控制器统一验证用户身份，并利用它访问网络资源，例如访问其他计算机上的共享文件夹、共享打印机等资源。

当用户利用域用户账户登录时，该账户数据会被送到域控制器，并由域控制器检查用户所输入的账户名和密码是否正确。

5.4.1　创建域用户

① 选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开活动目录管理工具。

② 如图 5-52 所示，右击“销售部”组织单元，在弹出的快捷菜单中选择“新建”→“用户”命令。

③ 如图 5-53 所示，在出现的“新建对象-用户”对话框，输入用户的姓名、用户的登录主名、用户的登录名。

④ 如图 5-54 所示，输入用户的密码 p@ssw0rd 和确认密码 p@ssw0rd，单击“下一步”按钮。该密

码包含了字符、特殊符号和数字，能够满足域的密码策略要求。

⑤ 单击“完成”按钮。

⑥ 如图 5-55 所示，可以看到在“销售部”组织单元的“用户”子组织单元中创建了“王瑞胜”用户账户。

⑦ 以同样的方式，在“研发部”组织单元的“用户”子组织单元中，创建“韩立刚”用户账户，登录主名为 hanLG@Ess.com，登录名为 ESS\hanLG；创建“张京铃”用户账户，登录主名为 zhangJL@Ess.com，登录名为 ESS\zhangJL。

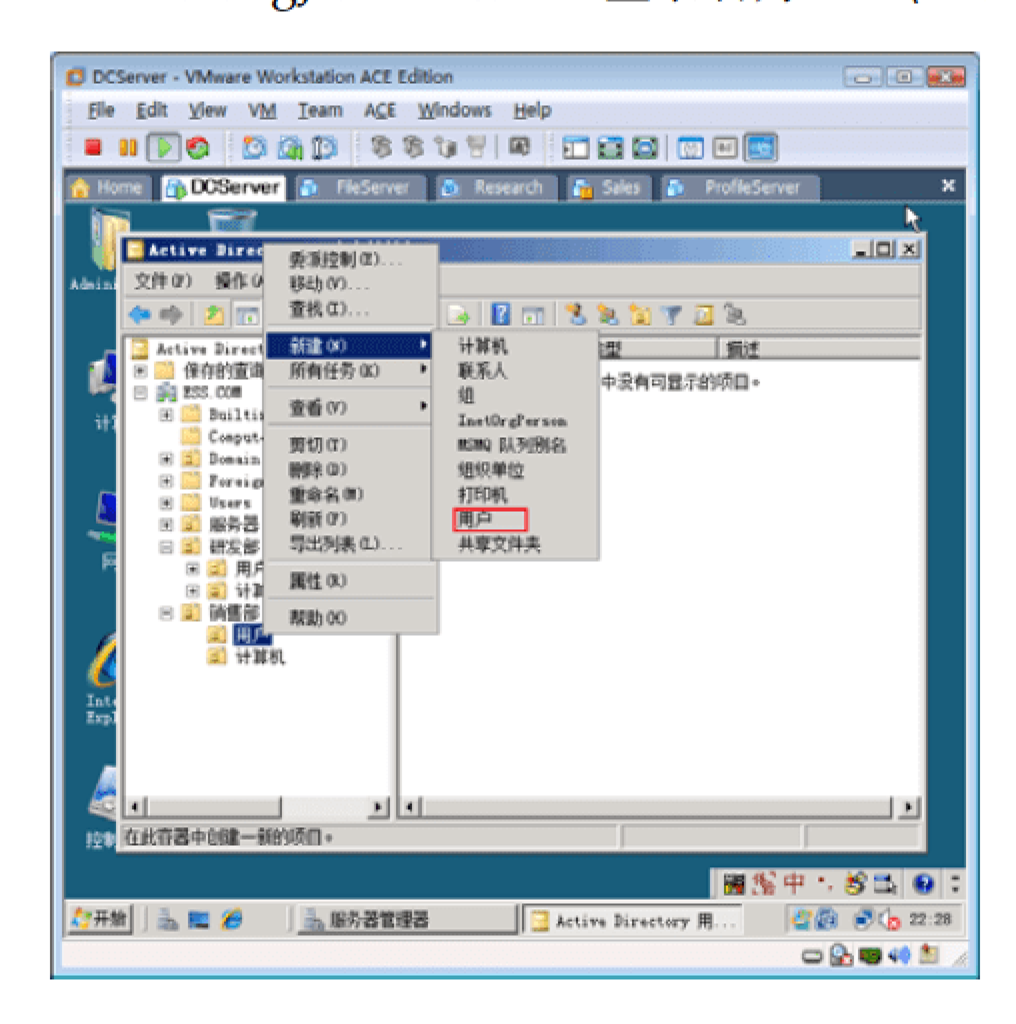


图 5-52　在销售部创建用户

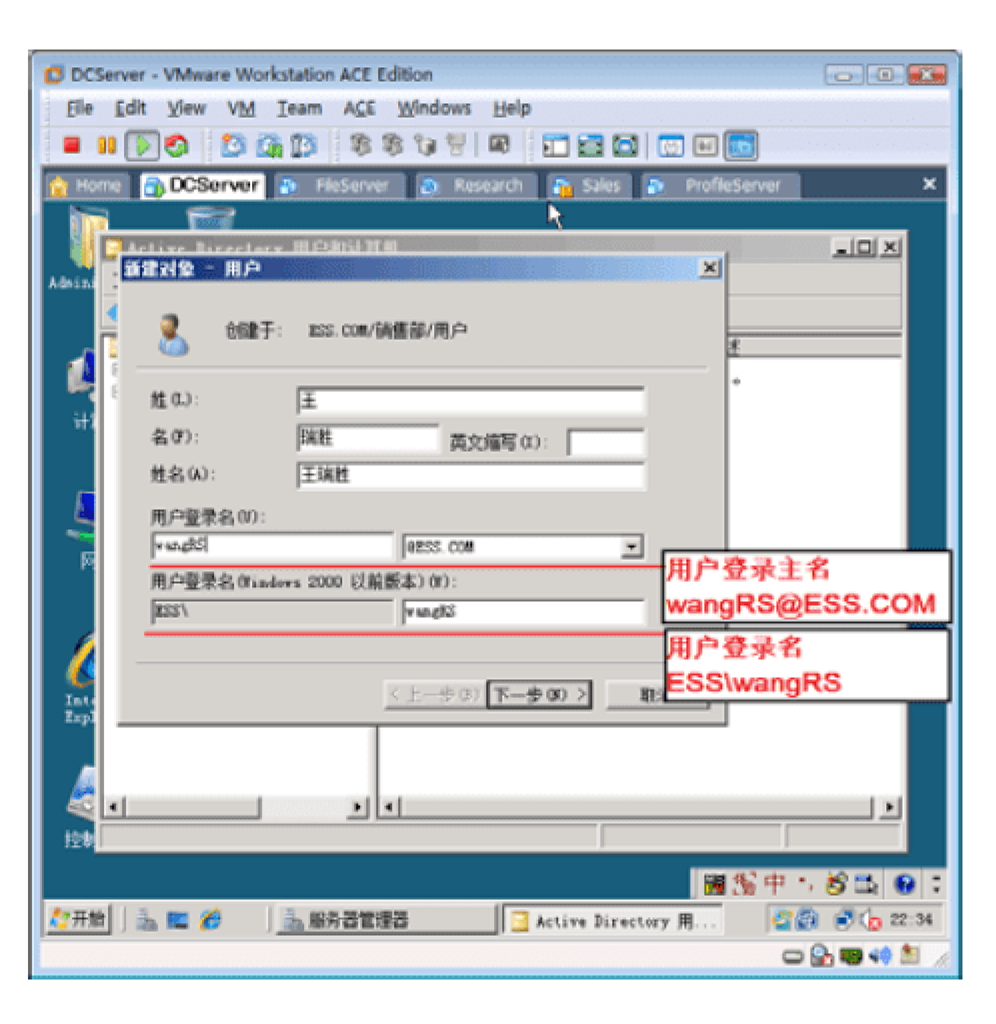


图 5-53　输入用户登录名和登录主名

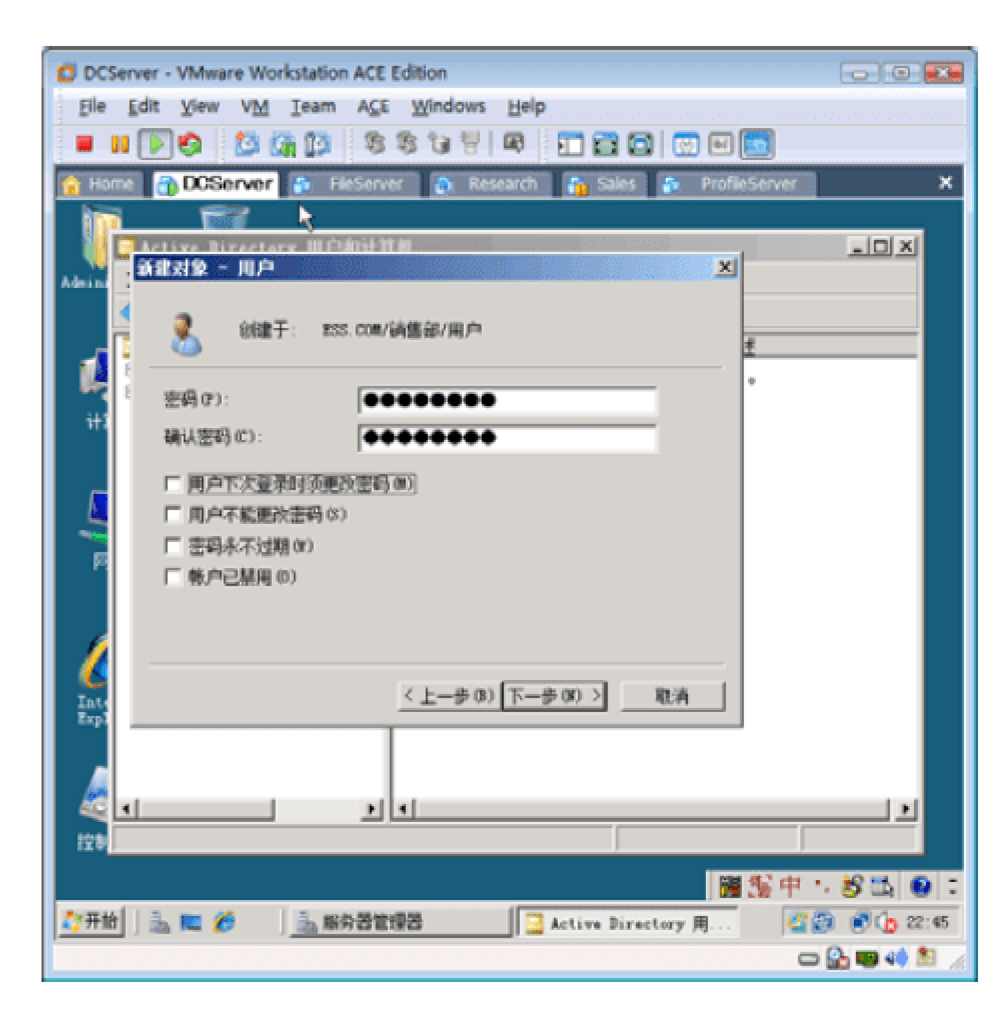


图 5-54　输入用户密码和确认密码

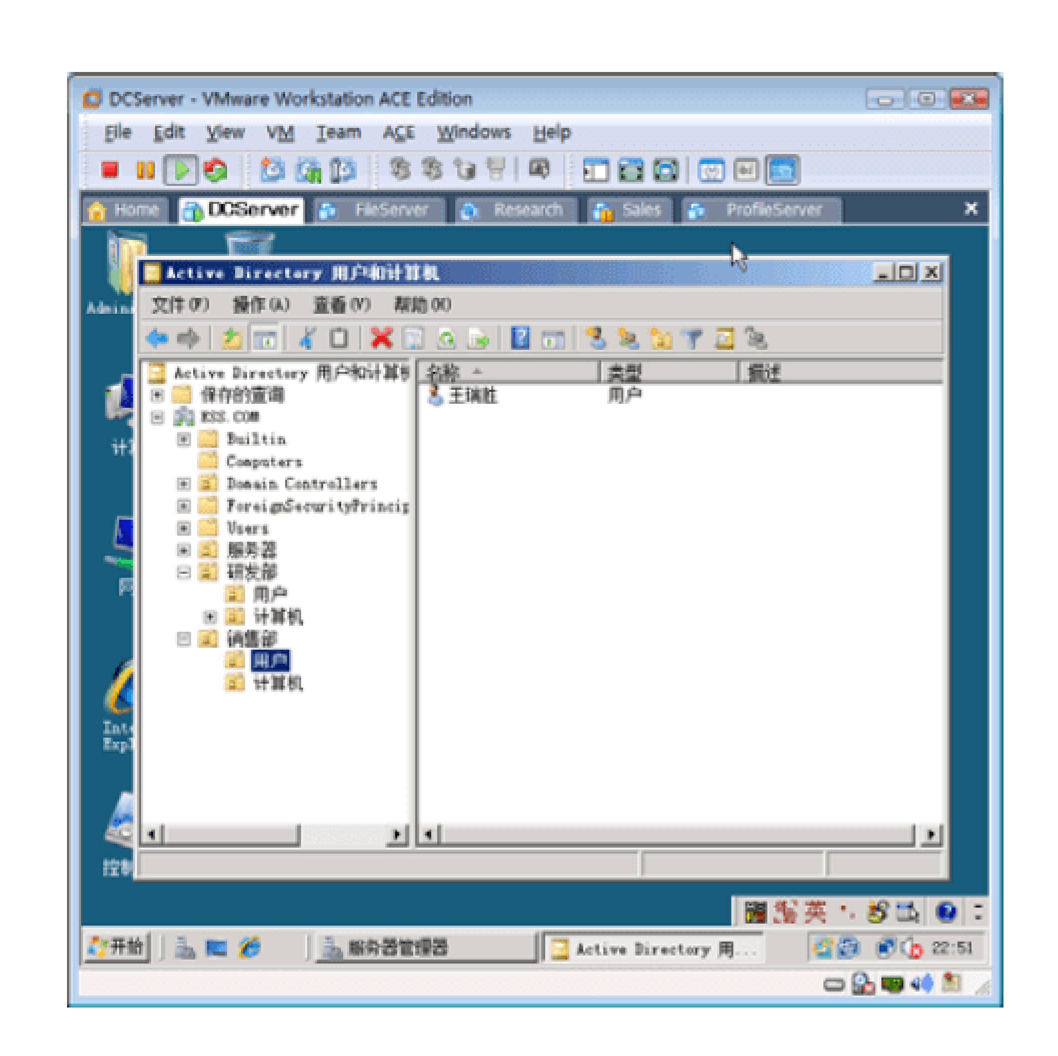


图 5-55　刚才创建的用户

5.4.2　域用户登录的方式

以下演示域用户使用登录名或登录主名在域中的计算机上登录。

① 销售部的域用户账户“王瑞胜”在销售部的计算机 Sales 上登录。

② 如图 5-56 所示，默认显示上次登录的账户，单击“切换用户”按钮。

③ 如图 5-57 所示，单击“其他用户”按钮。

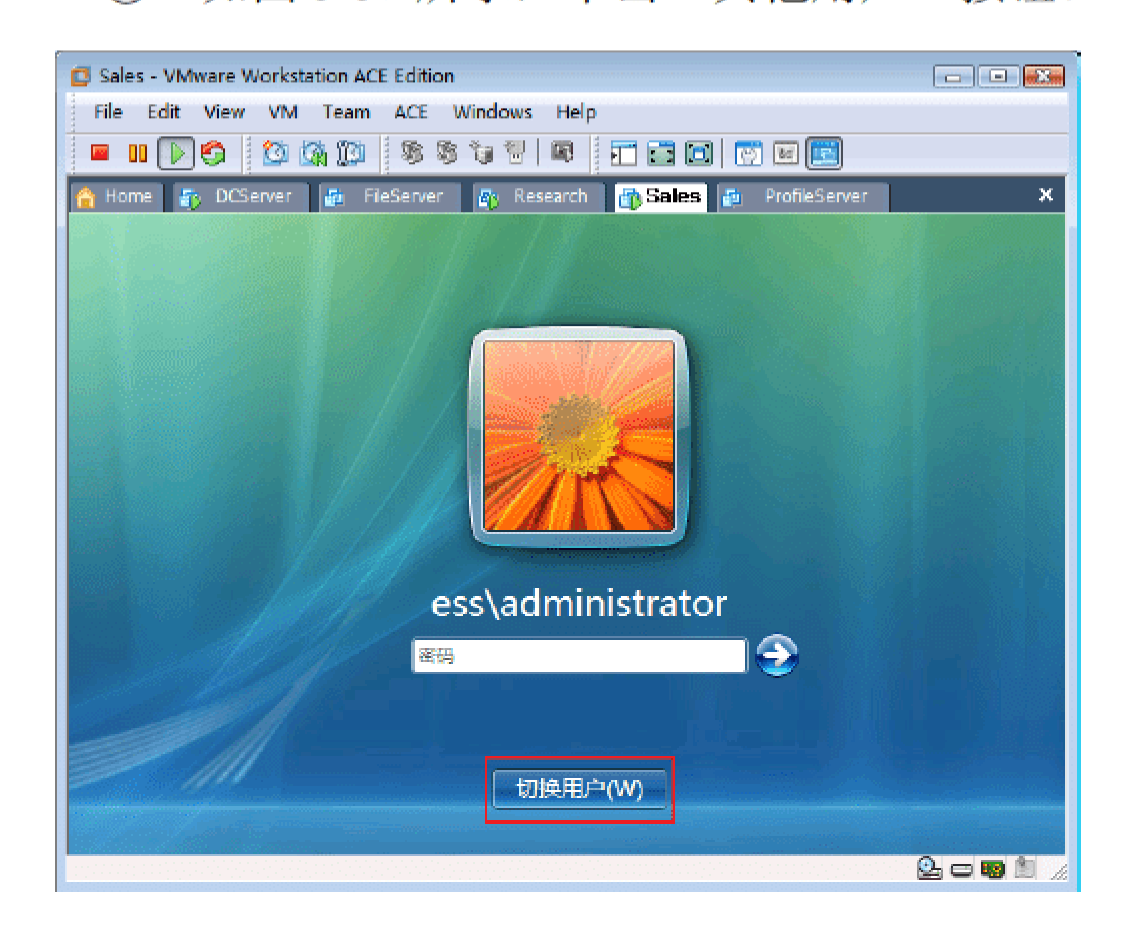


图 5-56　切换用户

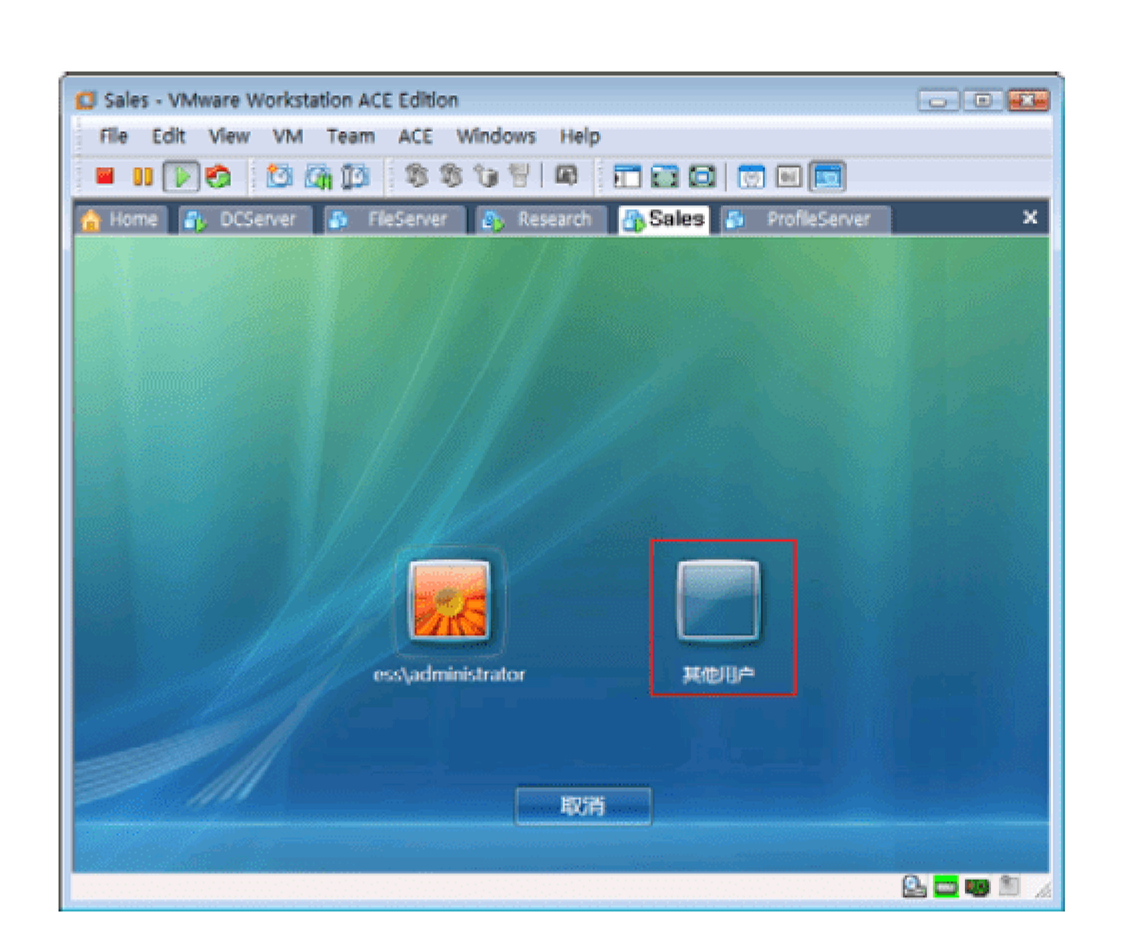


图 5-57　以其他用户登录

④ 如图 5-58 所示，使用登录名登录，输入 ESS\wangRS 和密码 p@ssw0rd，单击按钮登录。

⑤ 如图 5-59 所示，使用登录主名登录，输入 wangRS@Ess.com 和密码 p@ssw0rd，单击按钮登录。

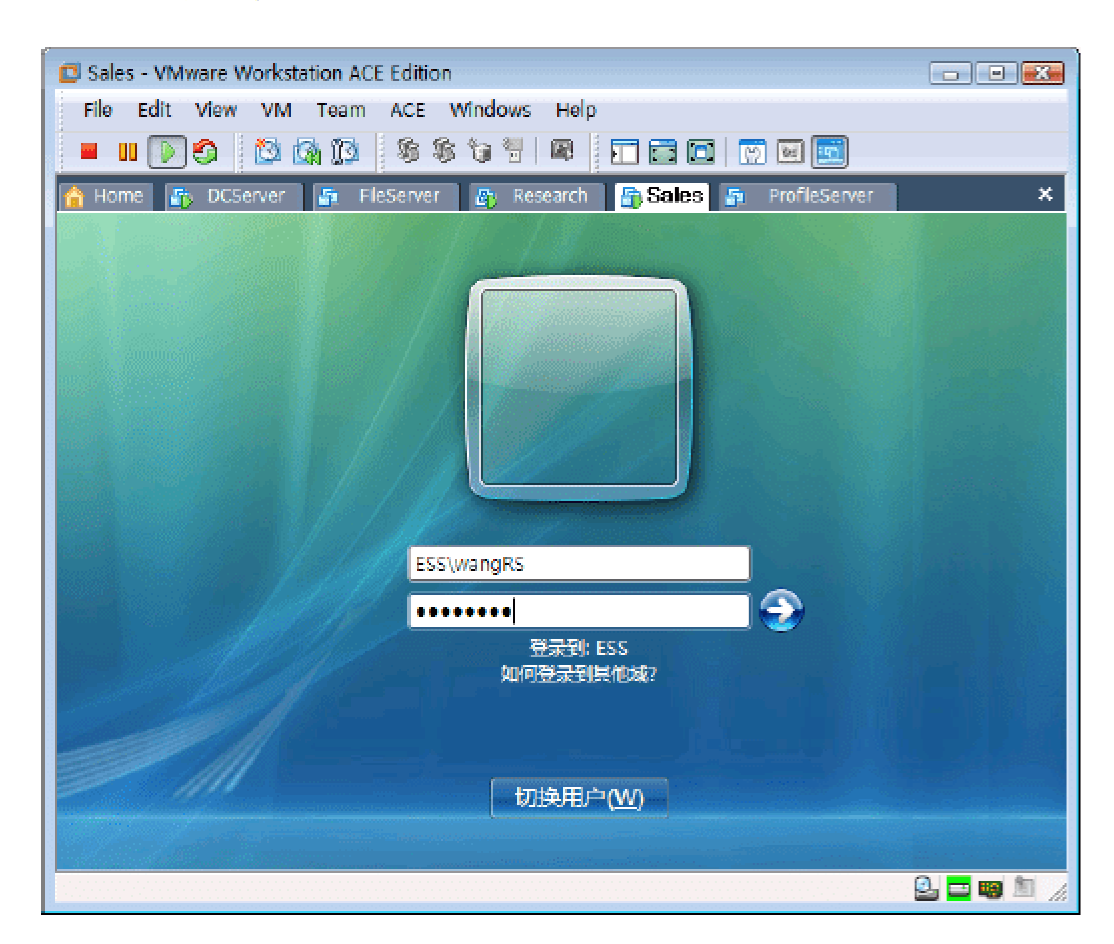


图 5-58　以登录名登录



图 5-59　以登录主名登录

5.4.3　重设域用户密码及用户自己更改密码

如果用户忘记了自己账户的密码，管理员可以重新设置用户密码。另外，用户也可以自己更改密码。

1. 任务

- 管理员重设用户密码。
- 用户自己更改密码。

2. 步骤

① 如图 5-60 所示，右击用户账号，在弹出的快捷菜单中选择“重置密码”命令。

② 如图 5-61 所示，输入新密码，如果想让用户自己管理自己的密码，则选中“用户下次登录时须更改密码”复选框。

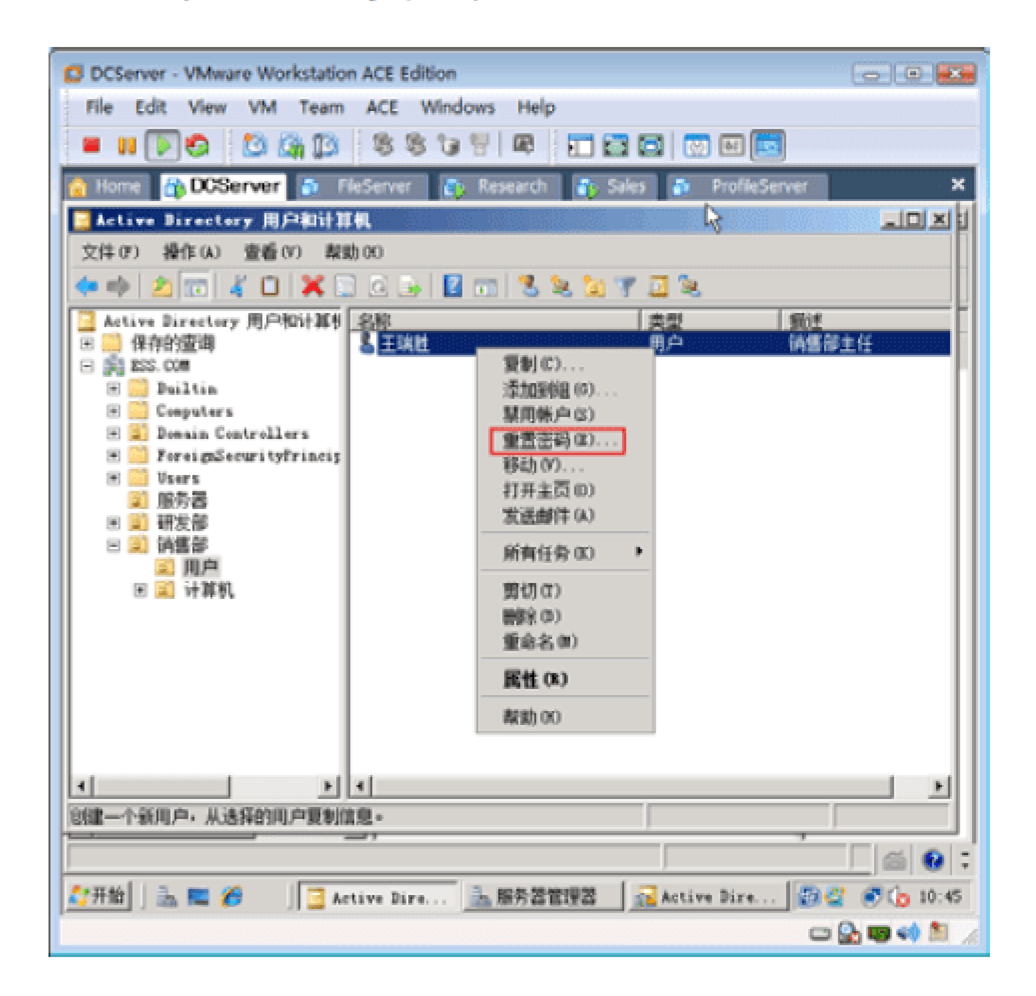


图 5-60 重设密码

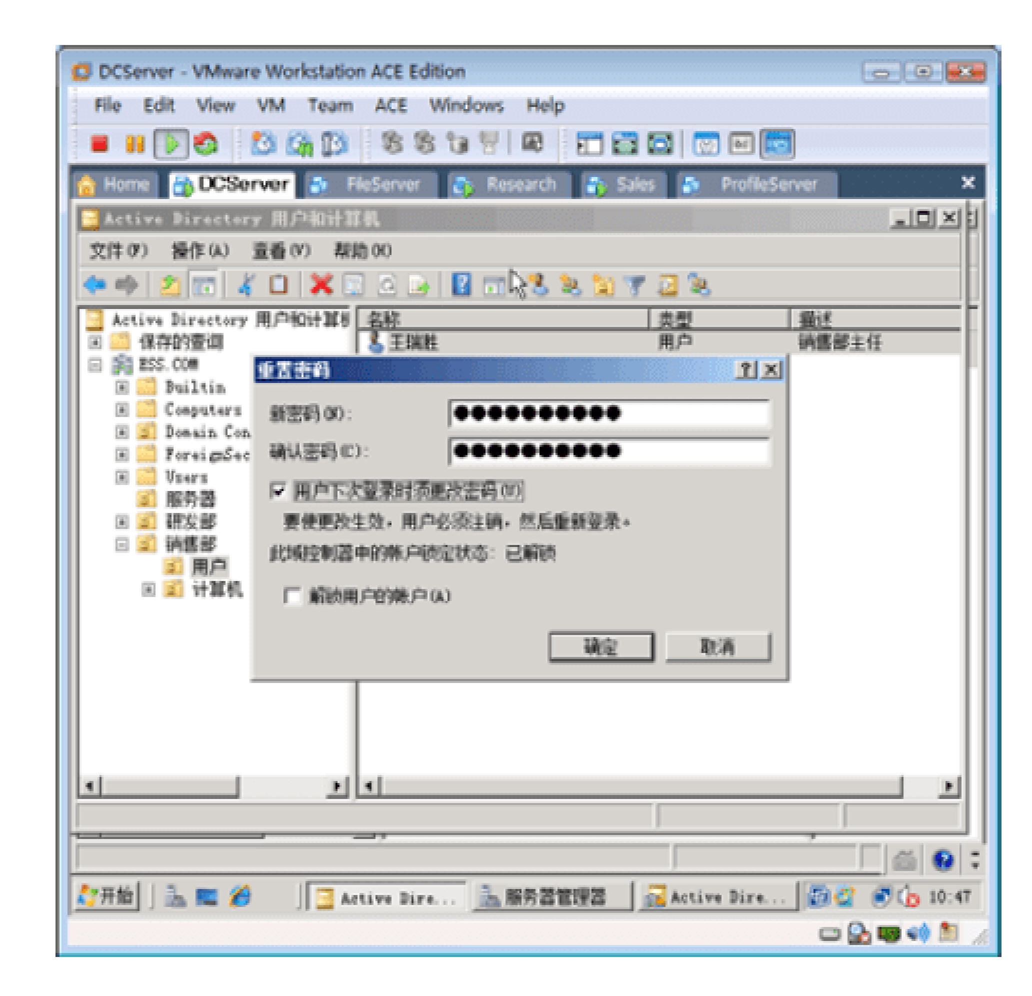


图 5-61 输入新密码和确认密码

③ 对于一些公共的账户或者服务账户，为防止个别人私自更改密码，造成其他用户不能登录或服务启动失败，可以双击用户账户，打开用户属性对话框，如图 5-62 所示，设置成用户不能更改的密码和密码永不过期。

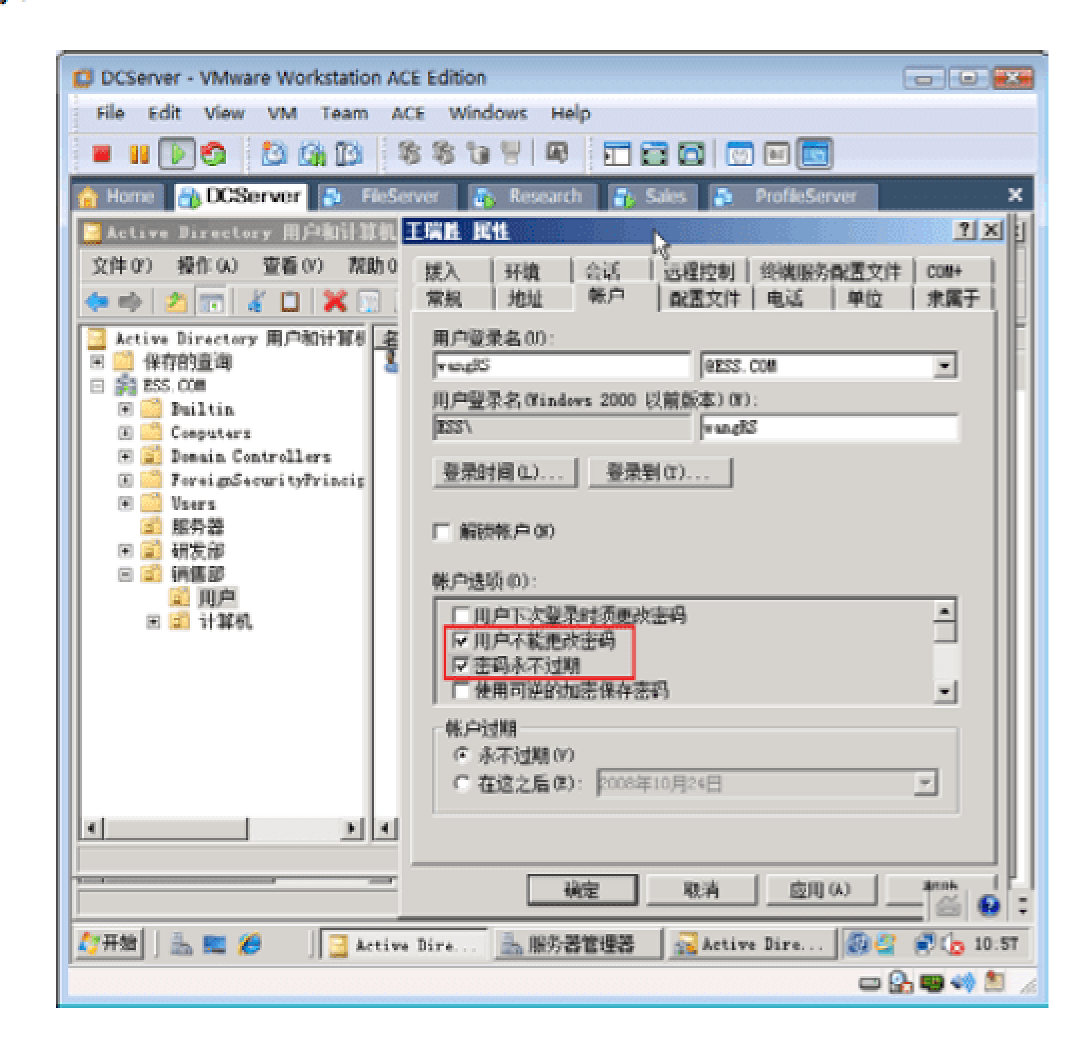


图 5-62 用户密码控制

④ 用户登录到域中的计算机后，按 Ctrl+Alt+Del 组合键，在虚拟机中按 Ctrl+Alt+Insert 组合键。

⑤ 如图 5-63 所示，单击“更改密码”按钮。

⑥ 如图 5-64 所示，输入旧密码，然后输入新密码并确认新密码，单击按钮，更改密码。

注意：默认域中安全策略，要求用户的密码至少使用 1 天，如果你的用户是刚刚创建的，你使用上面的方法更改密码会提示“无法更改密码。为新密码提供的值不符合字符域的长度、复杂性或历史要求”。

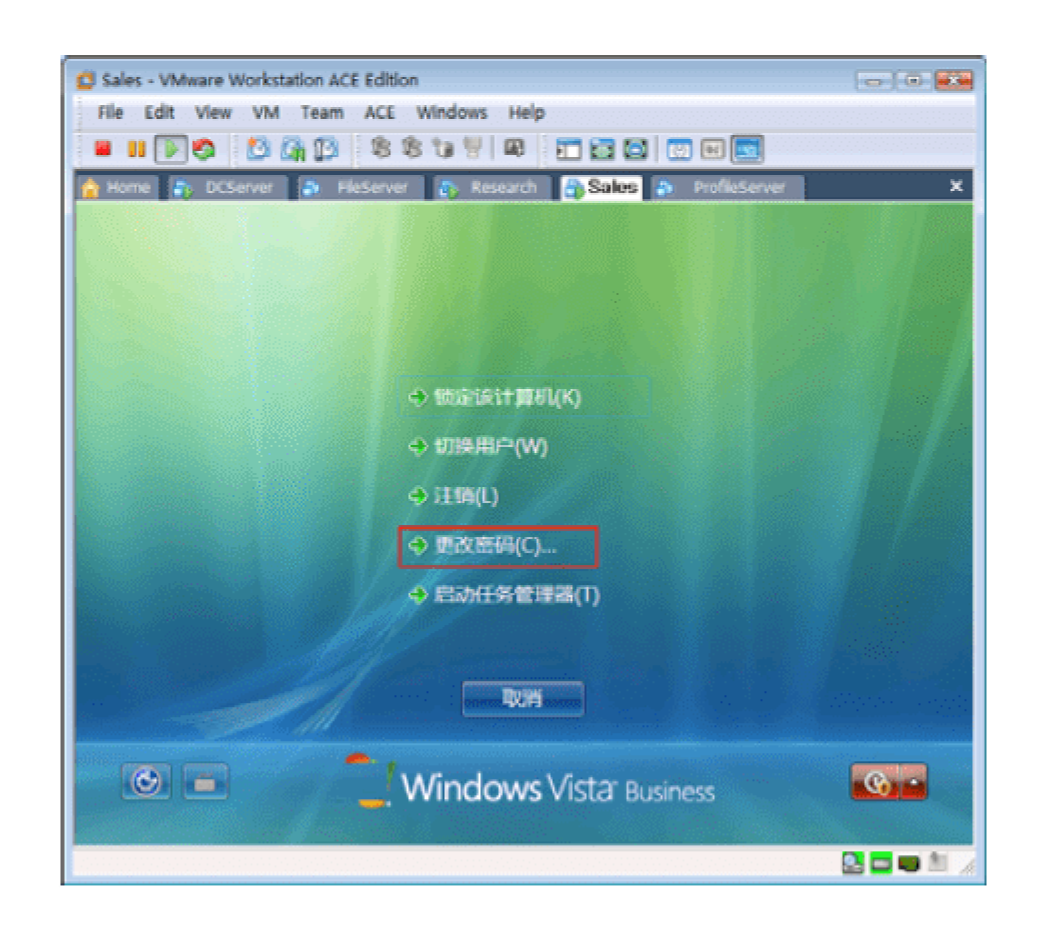



图 5-63　更改密码

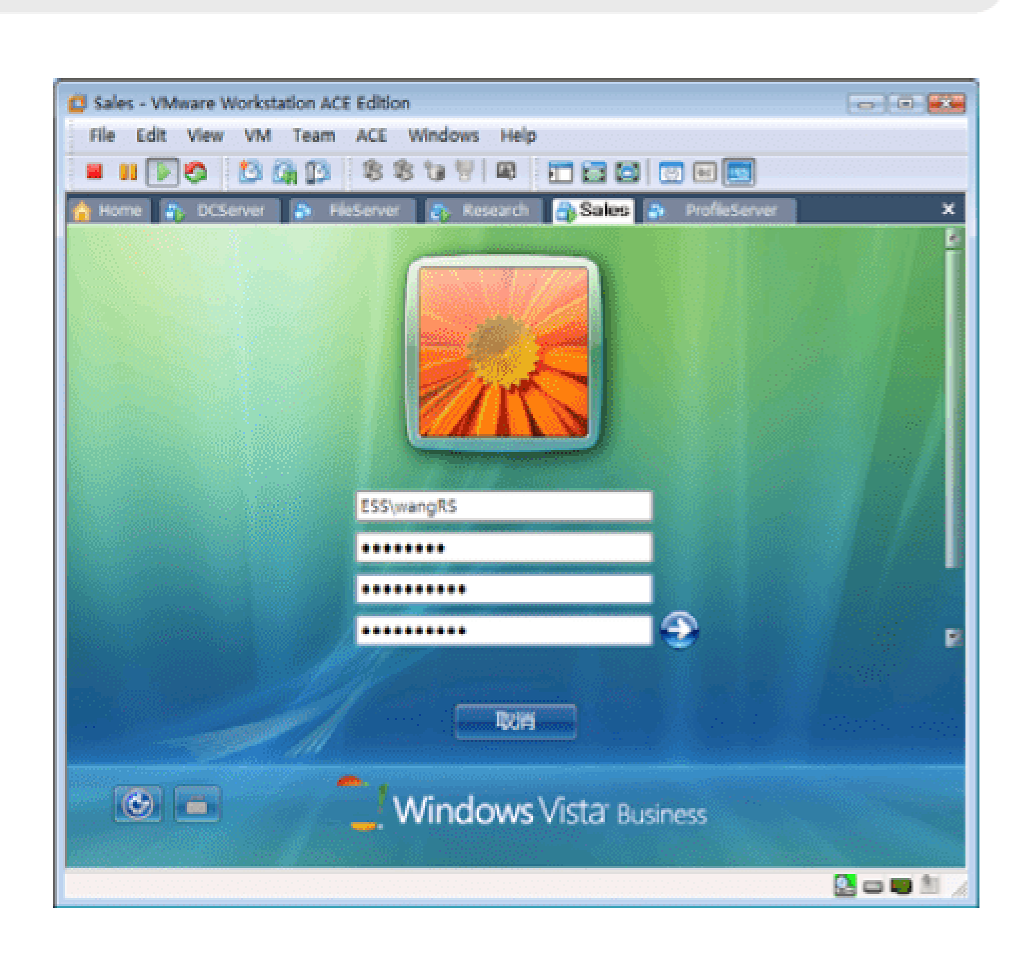


图 5-64　输入新旧密码

5.4.4　设置域用户账户的登录时间

“登录时间”用来设置用户什么时间可以登录到域。默认为用户可以在任何时间登录到域。

① 如图 5-65 所示，双击用户账户，在出现的用户属性对话框中，切换到“账户”选项卡，单击“登录时间”按钮。

② 如图 5-66 所示，可以指定用户能够登录到域的时间段，最小单位为小时。

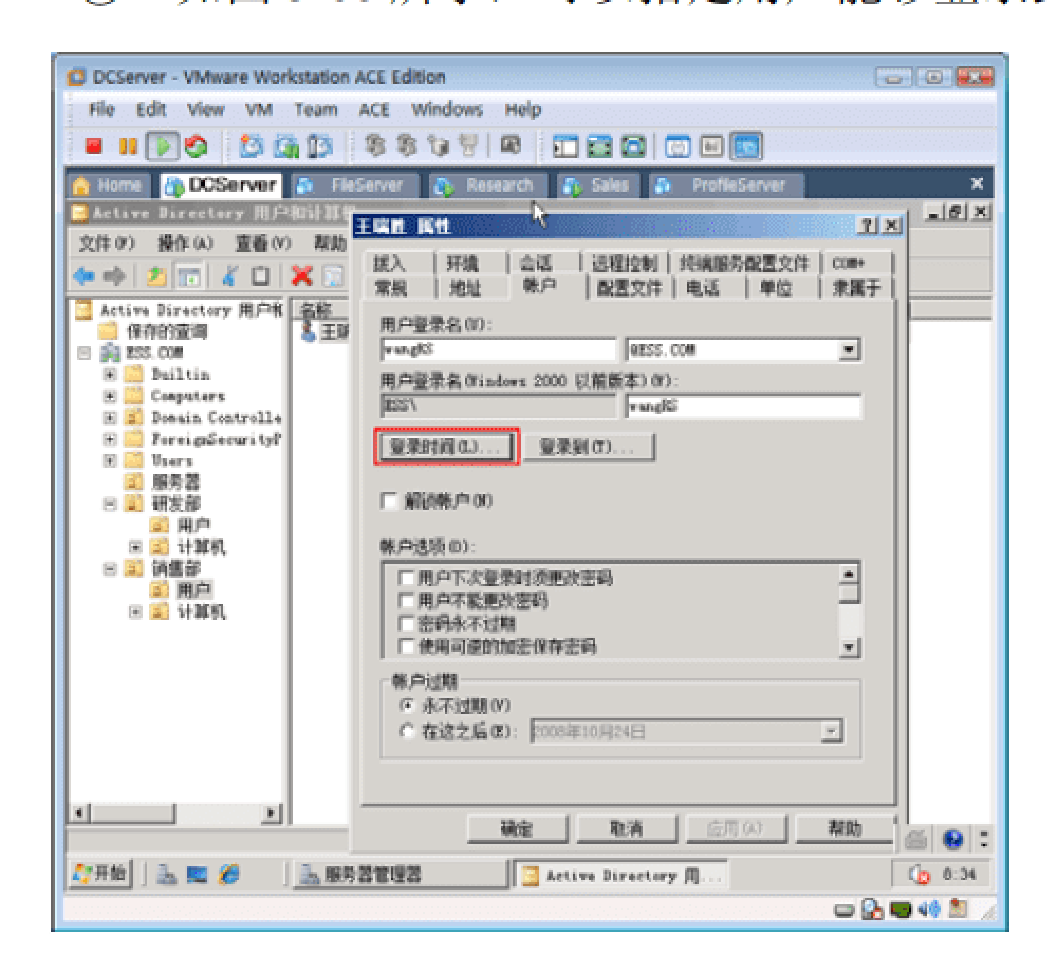


图 5-65　用户属性

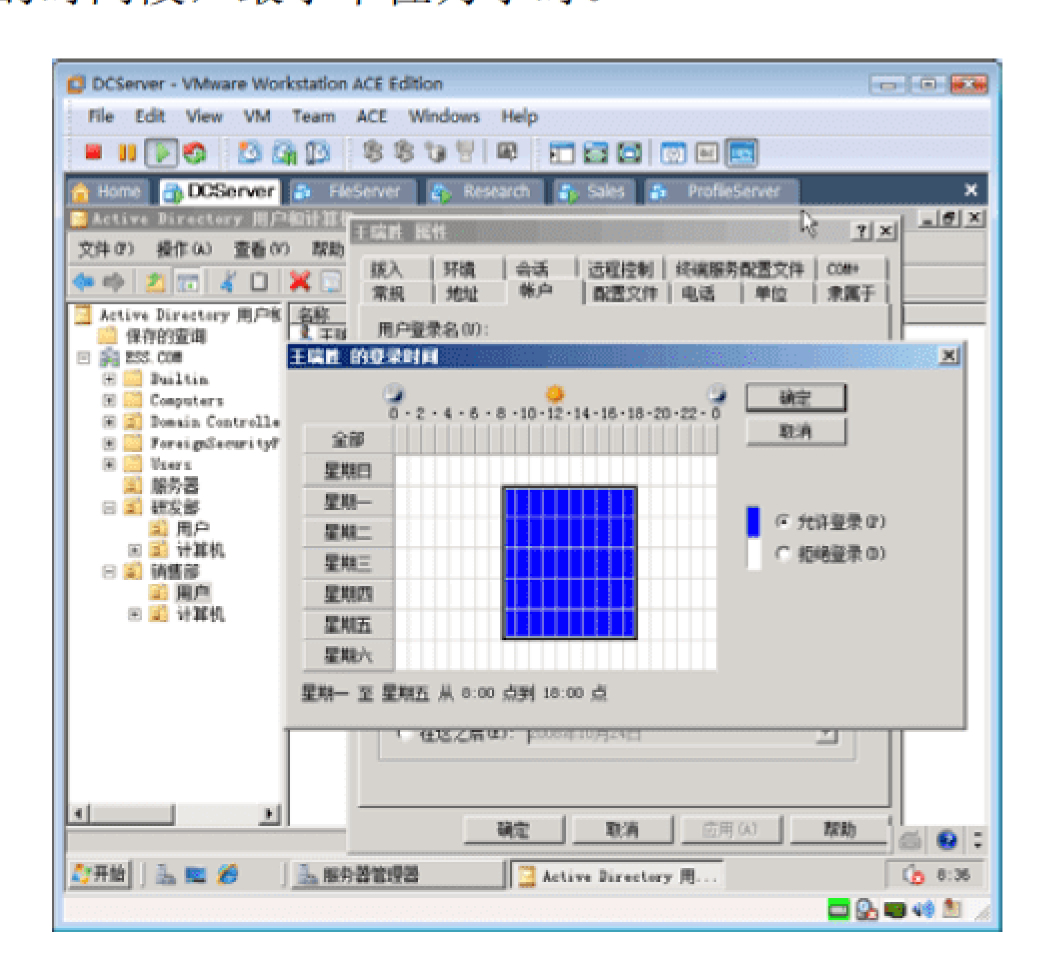


图 5-66　设置登录时间

如果用户登录没有在指定的时间段内登录，如图 5-67 所示，将会出现“您的账户有时间限制，您当前无法登录，请稍后再试”的提示。

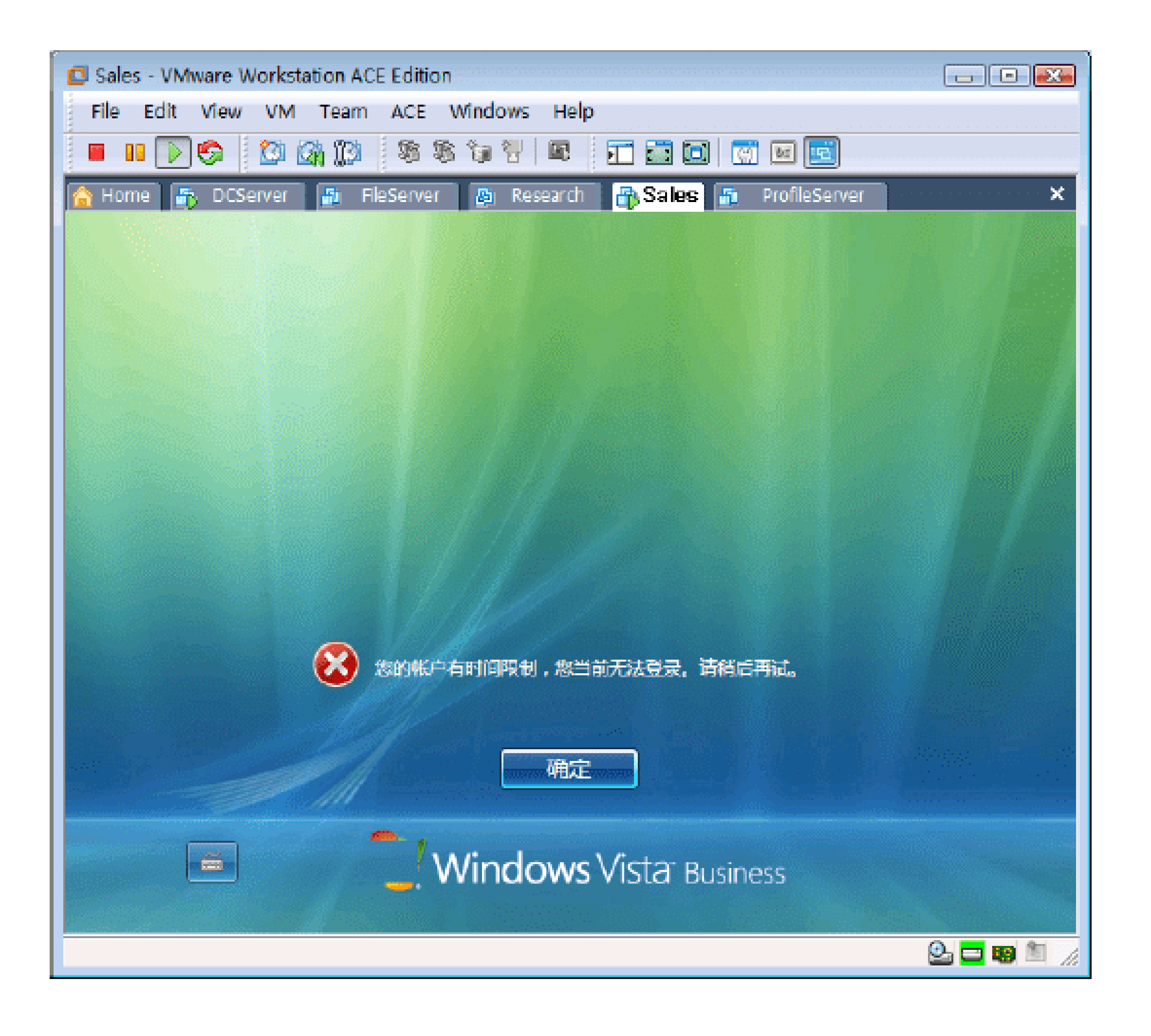


图 5-67　时间限制

5.4.5　设置域用户只能登录到特定的计算机

默认域用户可以登录域的成员计算机中的任何计算机，为了安全起见，可以指定域用户能够登录的计算机。

① 双击用户账户，在出现的用户属性对话框中，切换到“帐户”选项卡，单击“登录到”按钮，如图 5-68 所示，可以指定用户能够登录到域的那些计算机。

② 指定“王瑞胜”只允许在销售部门的计算机 Sales 上登录，如图 5-69 所示。

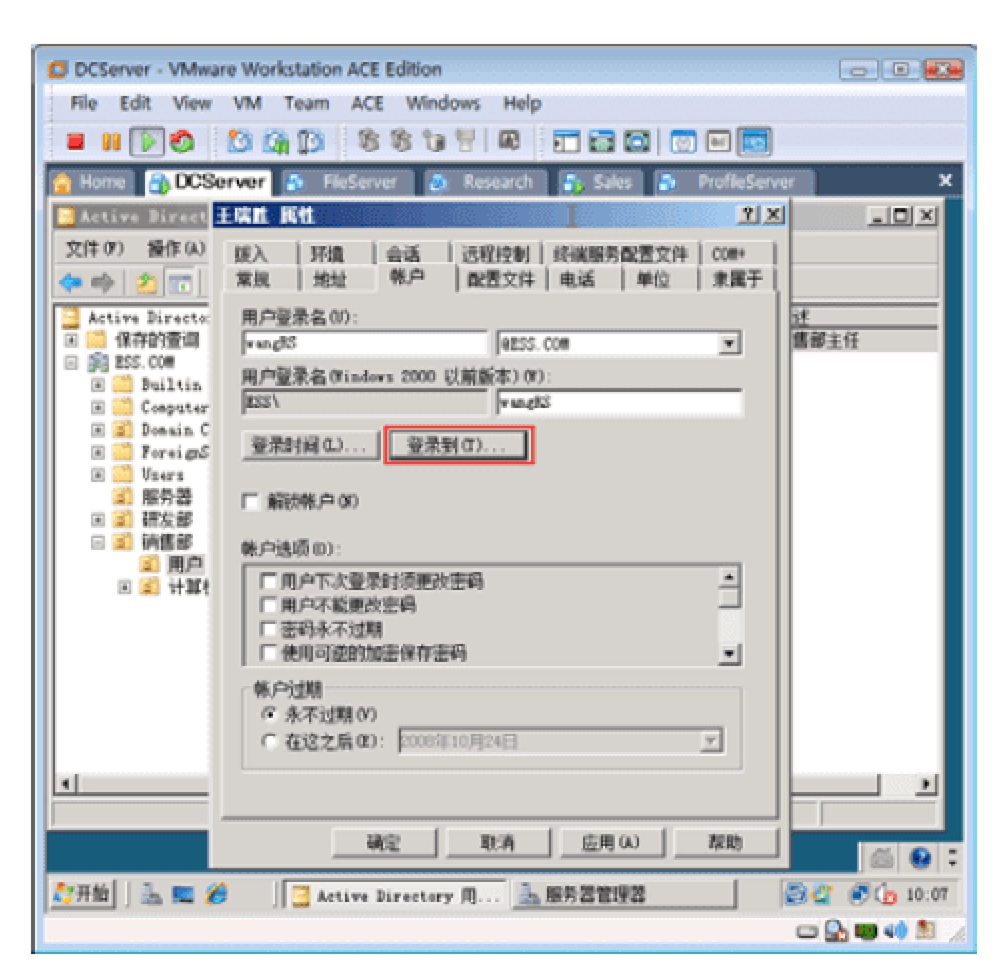


图 5-68　指定用户能够登录到的计算机

图 5-69　指定特定的计算机

③ 如图 5-70 所示，如果“王瑞胜”用户账户在研发部门的 Research 计算机上登录，将有“您的帐户配置为阻止您使用该计算机。请尝试其他计算机”的提示。

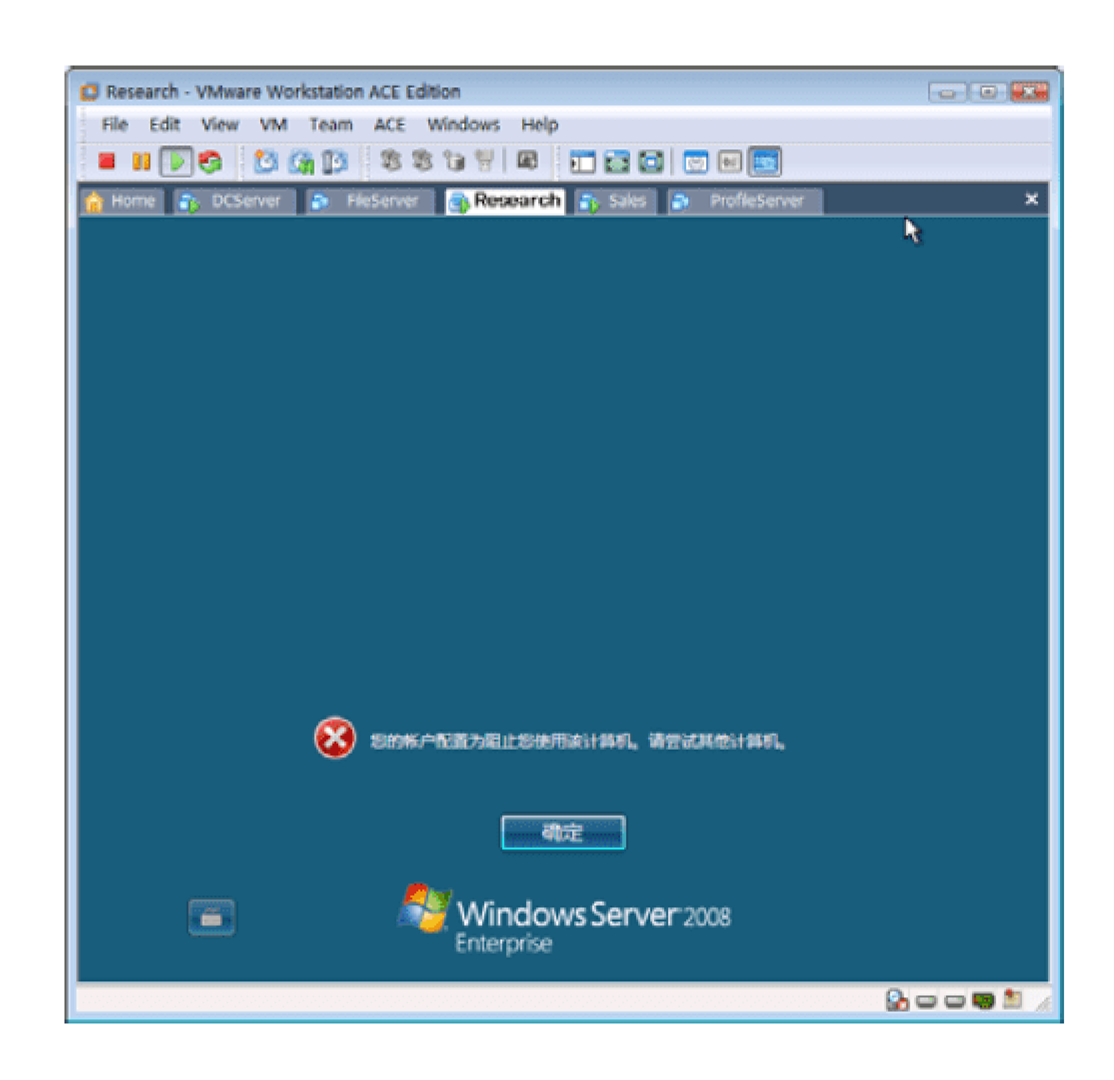


图 5-70　阻止用户使用某计算机

5.4.6　创建新的用户登录主名后缀

默认用户的登录主名后缀为域的名字，也可以创建新的域名后缀，这样就可以为不同部门的用户创建不同的登录主名后缀了。

① 如图 5-71 所示，选择“开始”→“程序”→“管理工具”→“Active Directory 域和信任关系”命令。

② 在打开的“Active Directory 域和信任关系”窗口中，如图 5-72 所示，右击“Active Directory 域和信任关系”选项，在弹出的快捷菜单中选择“属性”命令。

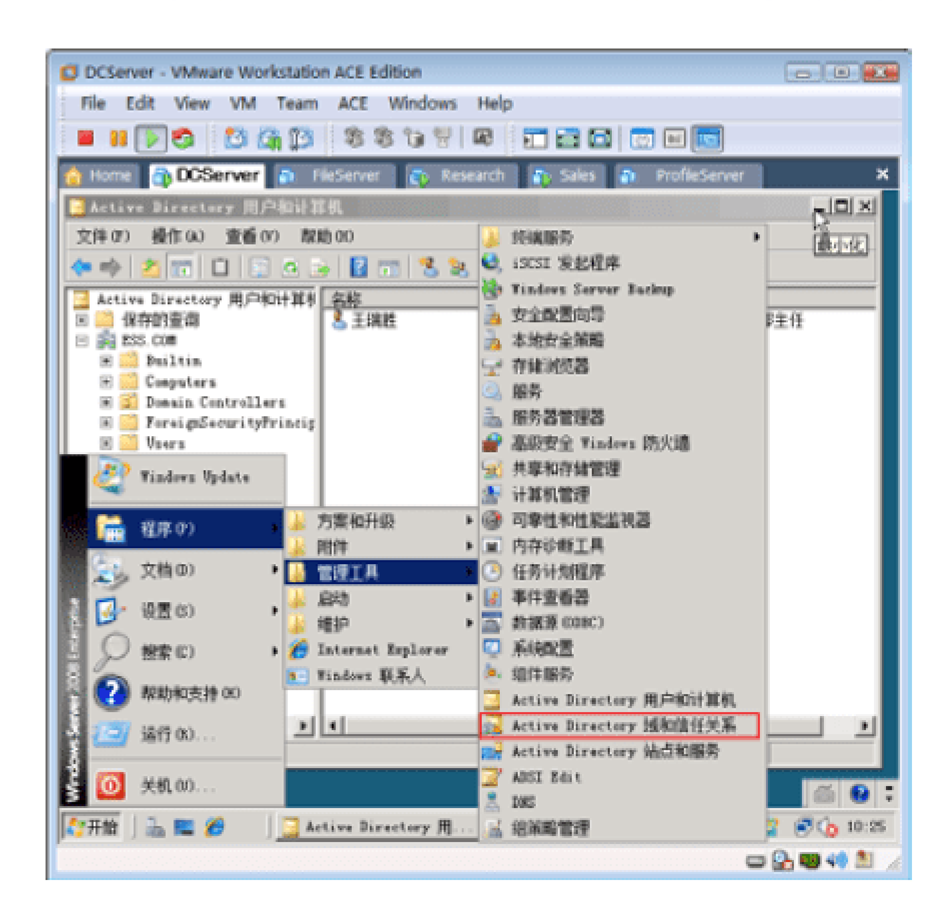


图 5-71　打开活动目录域和信任关系

图 5-72　选择属性

③ 如图 5-73 所示，可以为每个部门创建不同的登录主名后缀。

④ 如图 5-74 所示，再次打开“Active Directory 用户和计算机”窗口，双击销售部门的用户，在用户属性对话框中，切换到“帐户”选项卡，选中@Sales.com 选项，用户登录主名就变为 wangRS@Sales.com 了。

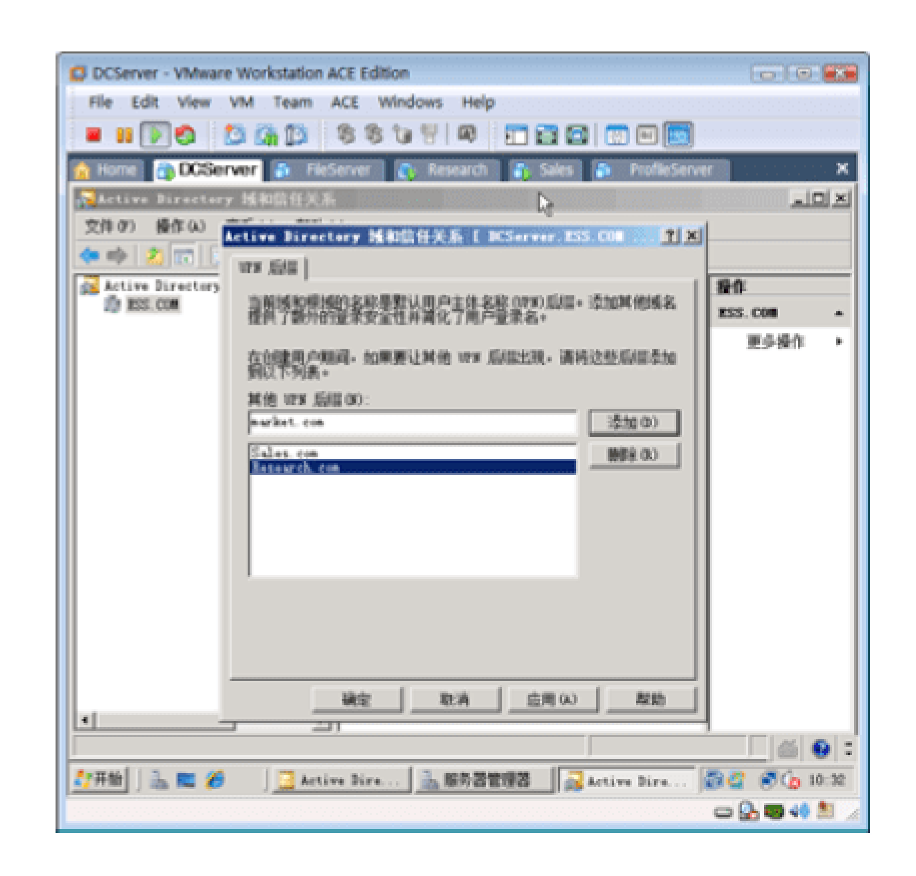


图 5-73　添加后缀

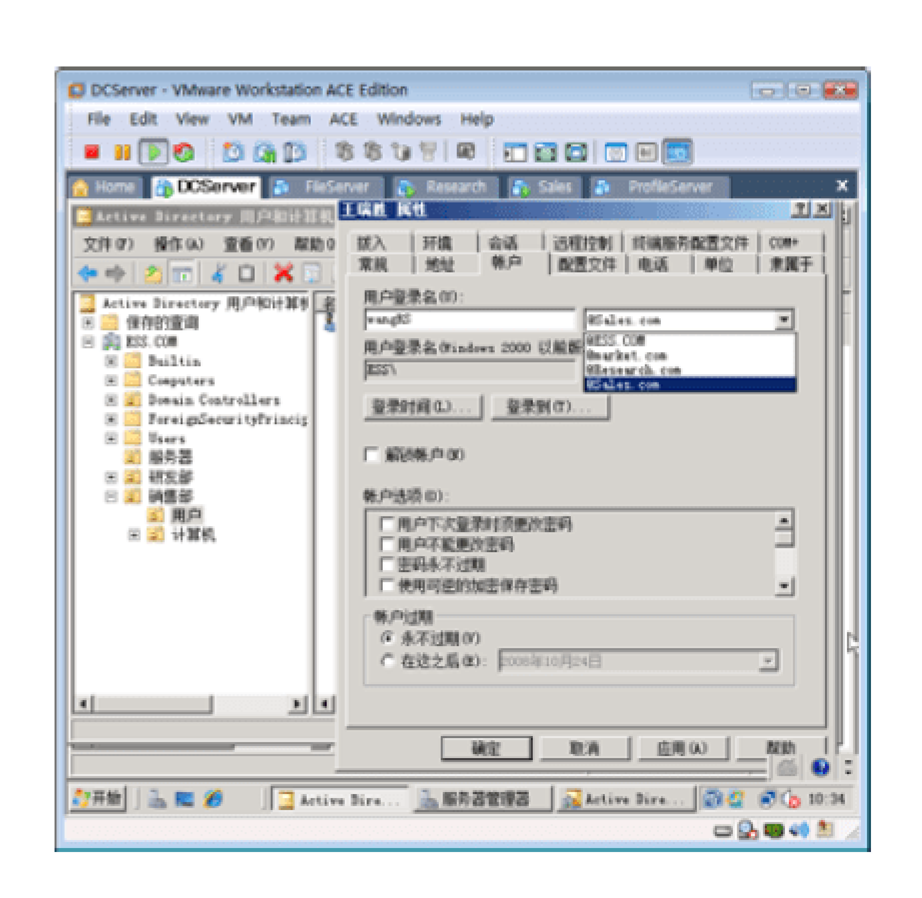


图 5-74　为用户指定后缀

5.4.7　设置用户登录主目录

用户主目录可以让域用户访问到网络上服务器上的共享目录。域用户在登录后会根据用户账户指定的主目录，自动为该用户映射一个网络驱动器。

以下步骤将会使销售部门的用户的主目录映射到服务器 FileServer 上的一个共享文件夹“公共空间”。

① 以域管理员的用户账户登录 FileServer。

② 在 FileServer 上创建一个共享文件夹“公共空间”，如图 5-75 所示，右击该共享文件夹，在弹出的快捷菜单中选择“共享”命令。

③ 如图 5-76 所示，在出现的“文件共享”对话框中，选中 Everyone 选项，单击“添加”按钮。

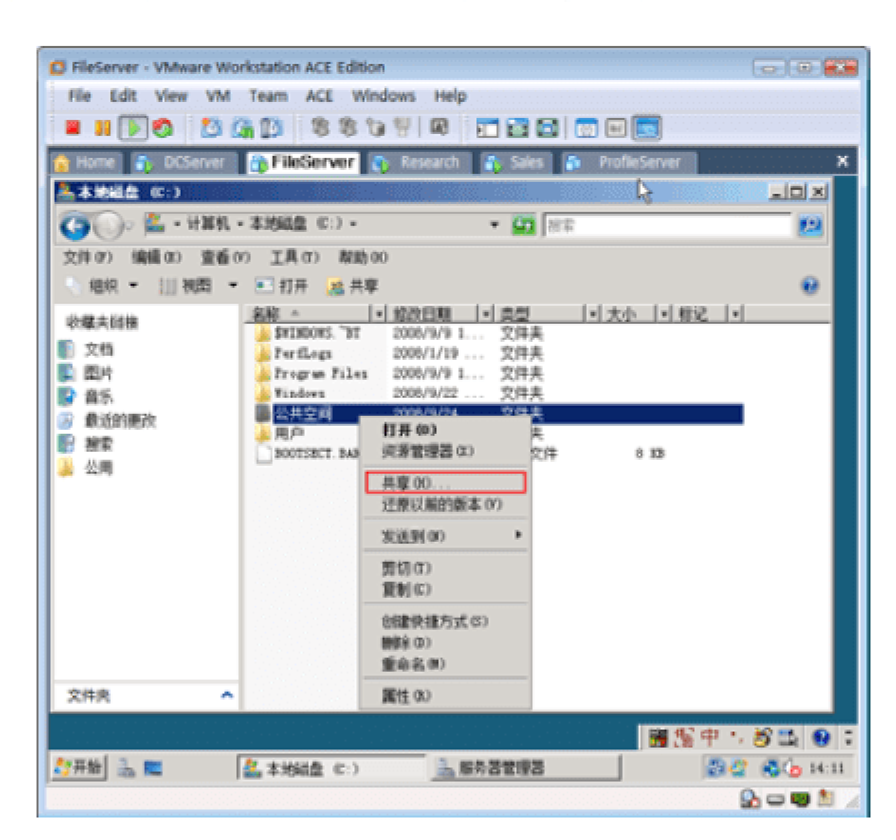


图 5-75　共享文件夹

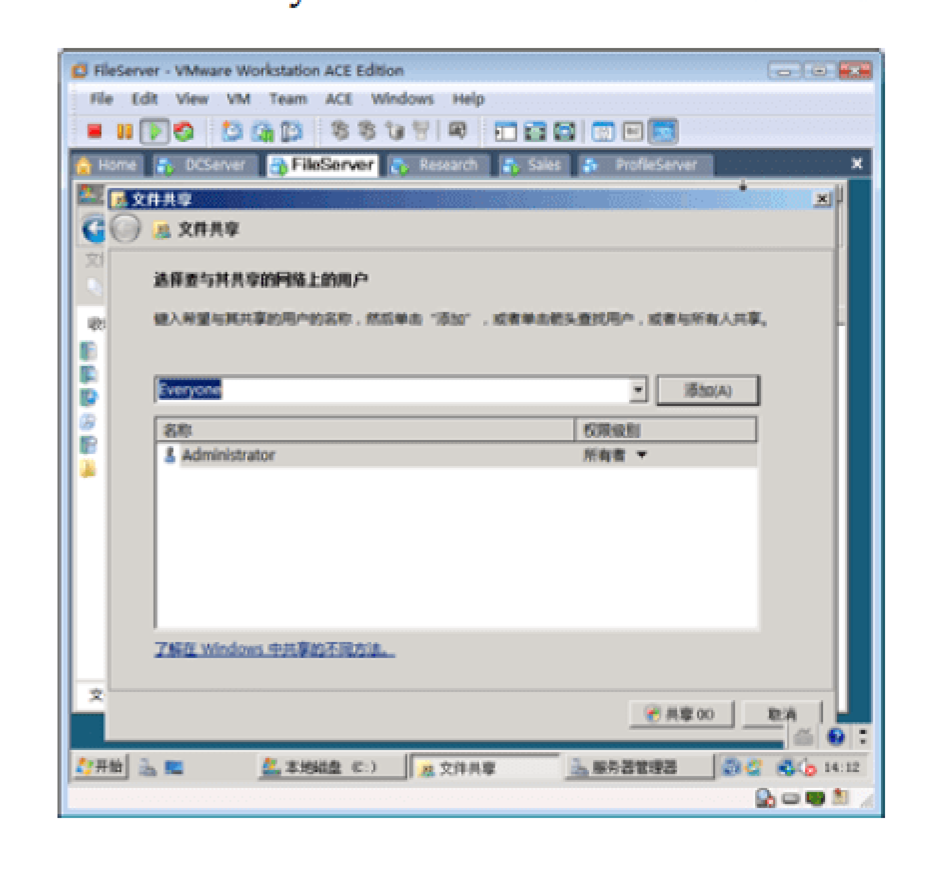


图 5-76　添加用户

④ 右击 Everyone 选项，在弹出的快捷菜单中选择“参与者”命令，单击“共享”按钮，如图 5-77 所示。

注意：“参与者”的权限能够使用户在共享的文件夹中添加/修改文件或文件夹。

⑤ 在 DCServer 服务器上，打开“Active Directory 用户和计算机”管理工具，如图 5-78 所示，同

时选中多个用户后右击，在弹出的快捷菜单中选择“属性”命令。

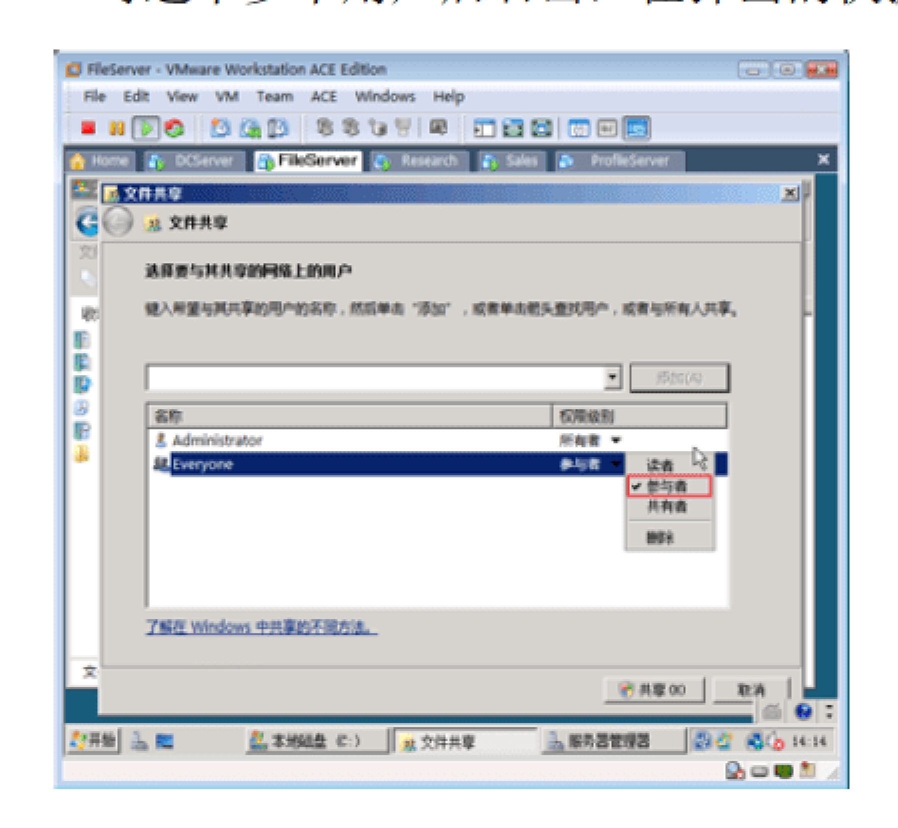



图 5-77　更改共享权限

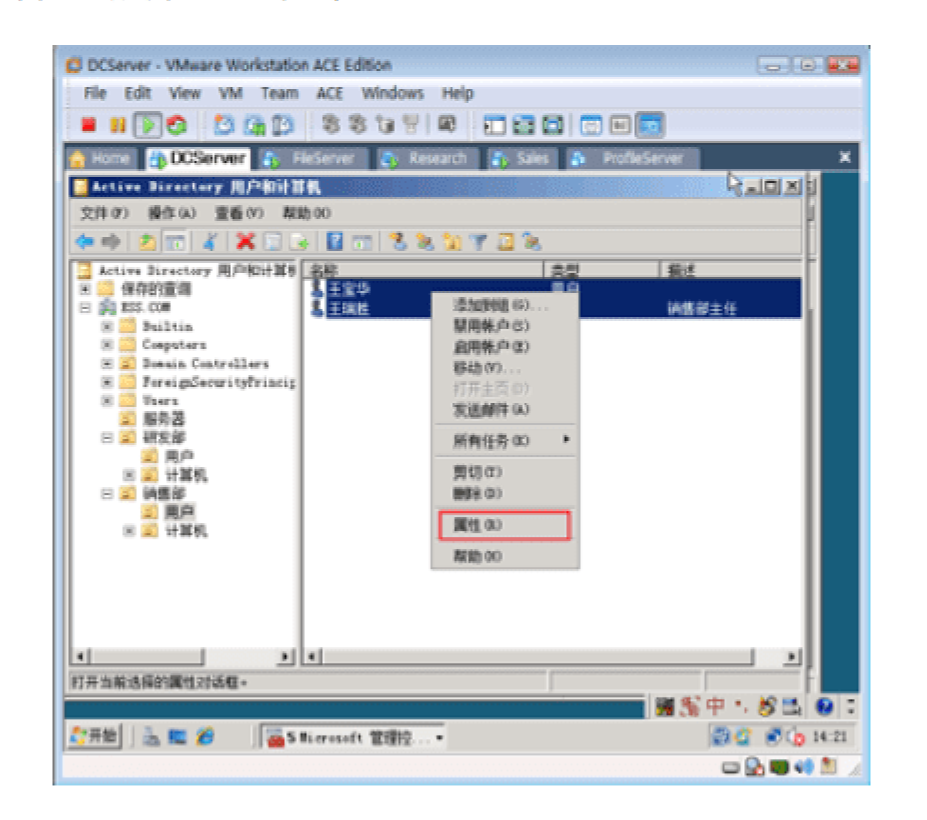


图 5-78　打开多个用户属性



提示：这种方式可以同时修改多个用户的属性。

⑥ 在多个用户属性对话框中，如图 5-79 所示，切换到“配置文件”选项卡。选中“主文件夹”复选框，选中“连接”单选按钮，盘符为 Z，位置为\\fileServer\公共空间\%username%，单击“确定”按钮。

注意：其中%username%是参数，会自动以账户的登录名替代。这样会自动在“公共空间”文件夹中自动以用户的登录名创建一个文件夹。

⑦ 使用“王瑞胜”账户在 Sales 计算机上登录。双击桌面上的“计算机”图标，能够看到自动映射了一个网络驱动器，如图 5-80 所示。

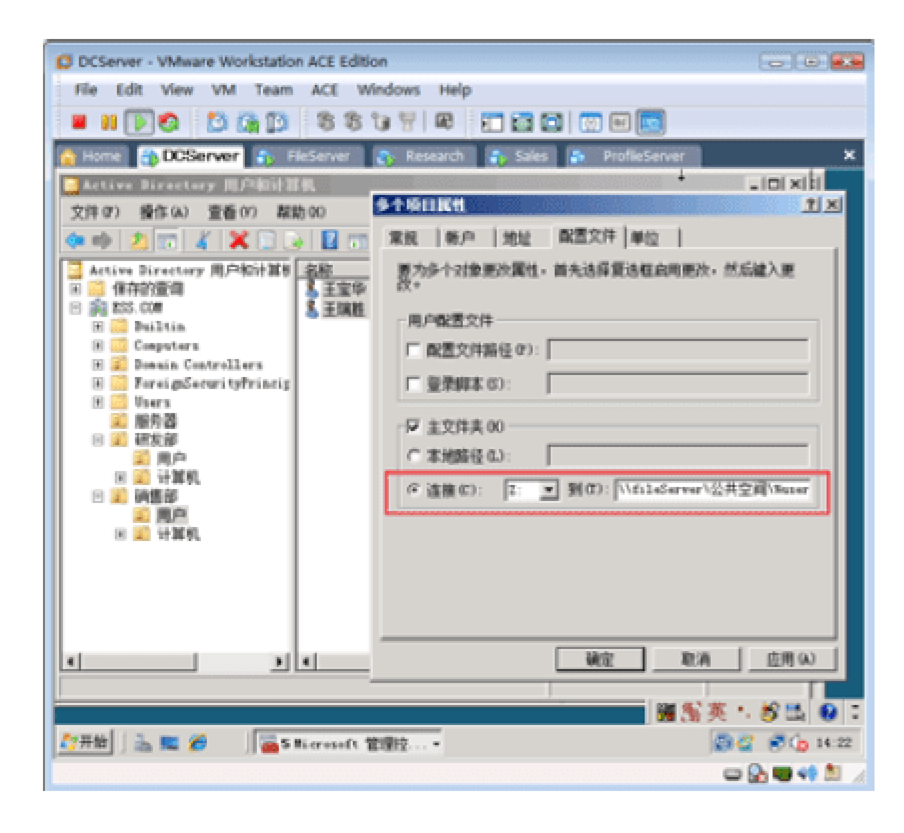


图 5-79　指定用户主文件夹

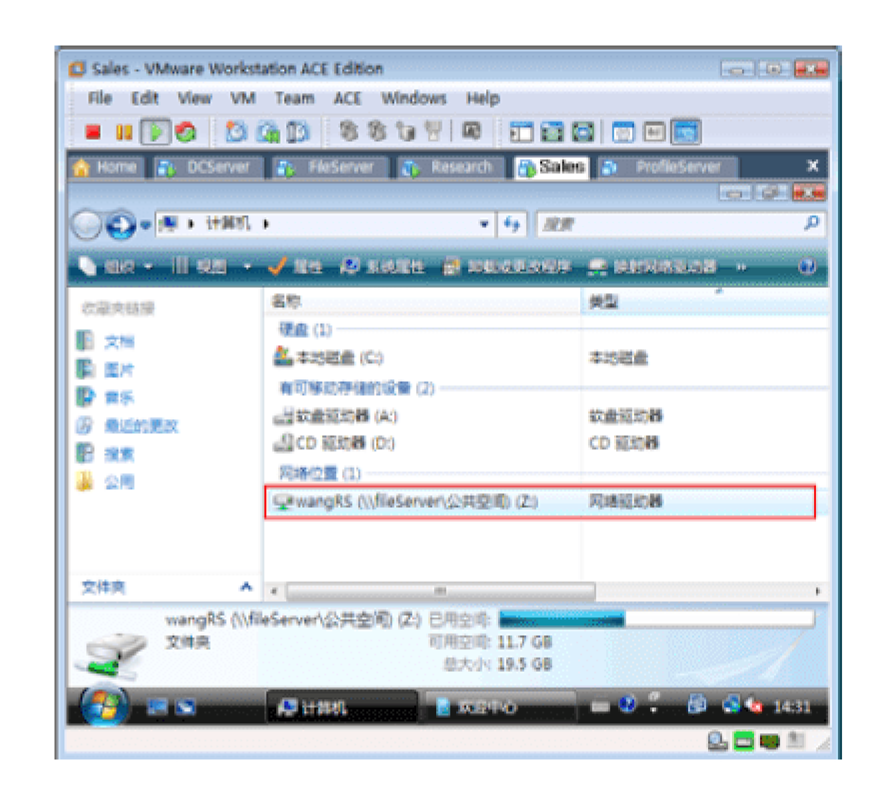


图 5-80　查看和使用主文件夹

5.4.8　使用保存的查询

保存的查询为管理员提供了一种快速、一致的方法，用来访问要对其执行特定任务或进行监视的一组

公共目录对象。保存的查询使用预定义的 LDAP 字符串仅搜索指定的域分区，搜索的范围可具体到单个容器对象。还可以创建自定义保存的查询，其中包含 LDAP 搜索筛选器。

可以保存查询以搜索禁用的用户或计算机账户、上次用户登录以后的天数、具有不过期密码的用户，以及许多其他常用查询。当执行保存的查询并显示出所需对象之后，每个对象都可以直接通过查询结果屏幕进行修改。此时，可以选择多个对象并对它们执行某项任务。例如，可使用拖放操作将两个或多个显示的对象放到一个组中。

以下的操作将演示如何创建一个查询，来找到销售部的用户账户。

① 在 DCServer 上，打开“Active Directory 用户和计算机”管理工具。

② 如图 5-81 所示，右击“保存的查询”，在弹出的快捷菜单中选择“新建”→“查询”命令。

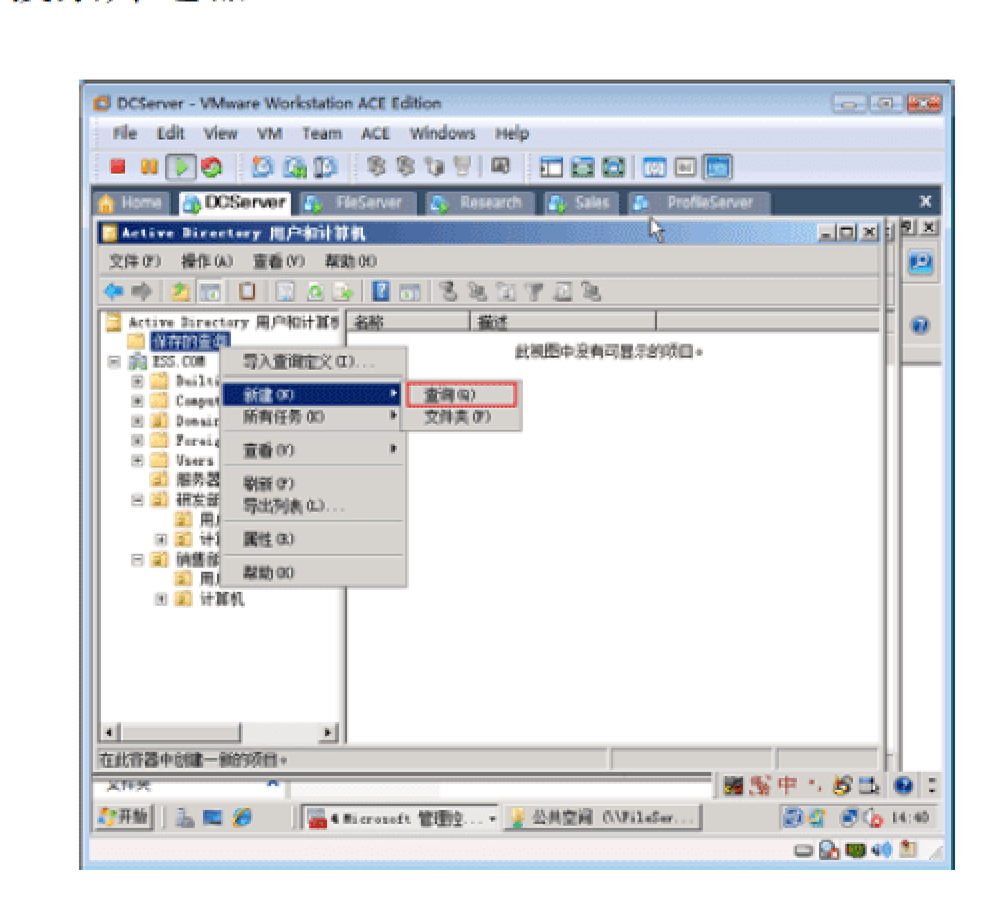


图 5-81　新建查询

③ 如图 5-82 所示，在“新查询”对话框中，输入名称“销售部员工”，单击“定义查询”按钮。

④ 如图 5-83 所示，在出现的“查找 用户、联系人及组”对话框中，选择“用户、联系人及组”选项。

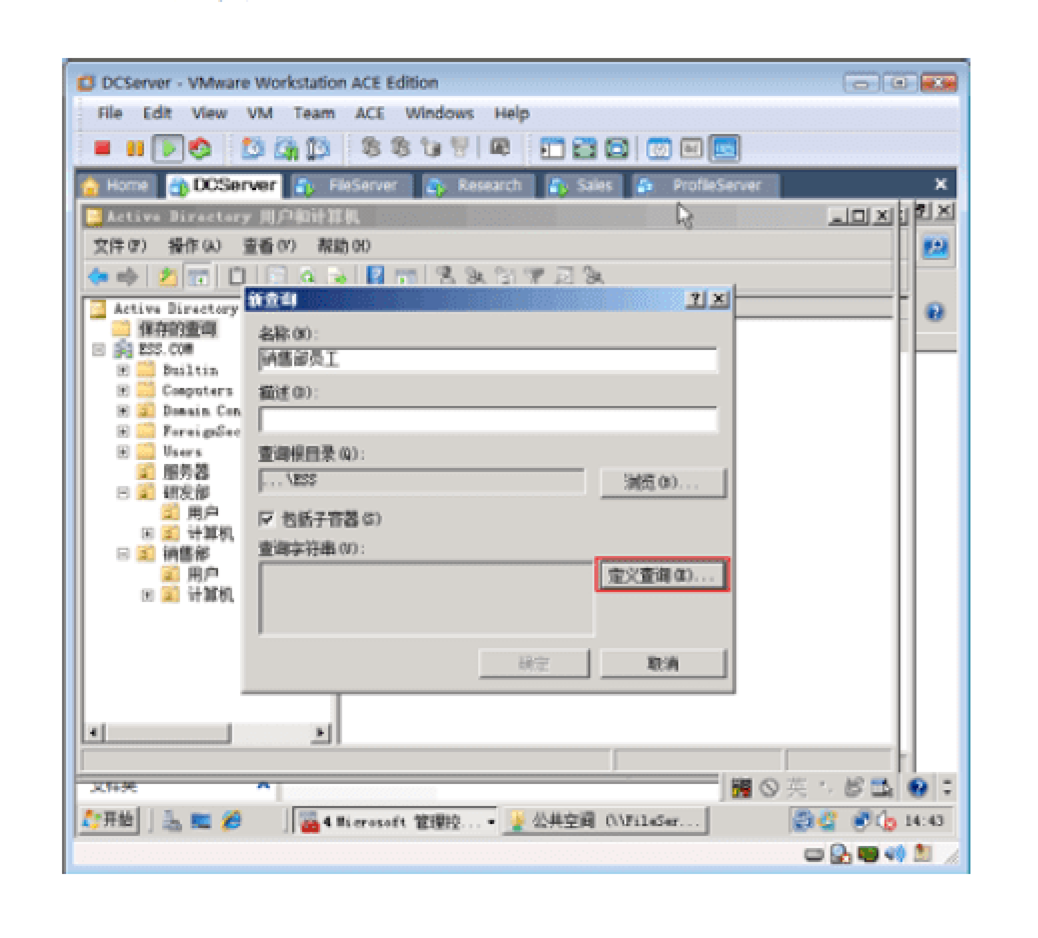


图 5-82　输入查询名称

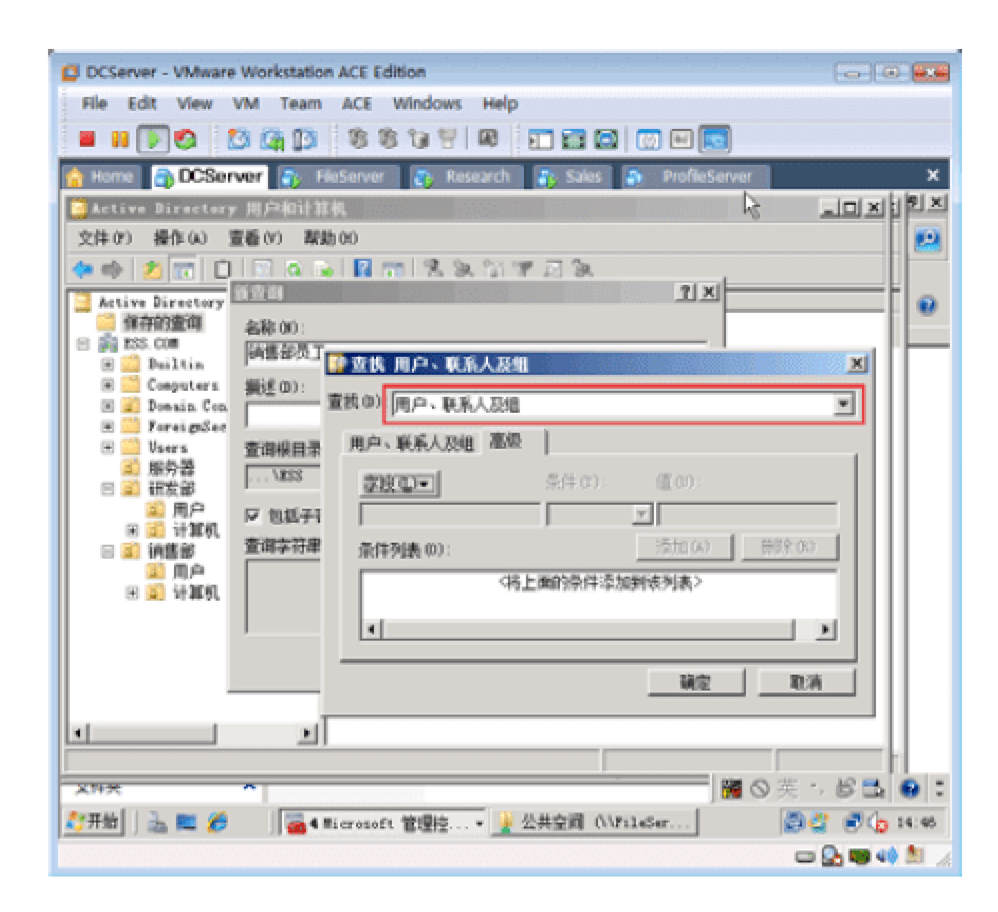


图 5-83　选择查询类型

⑤ 如图 5-84 所示，指定查询条件为“部门”。

⑥ 如图 5-85 所示，输入“销售部”，单击“添加”按钮，然后单击“确定”按钮。



提示：当然你还可添加多个查询条件。

⑦ 如图 5-86 所示，会自动生成查询语句，单击“确定”按钮。

⑧ 如图 5-87 所示，查看查询的结果，现在能够看到两个用户账户。

⑨ 如图 5-88 所示，在“刘强”账户部门属性中输入“销售部”，单击“确定”按钮。

⑩ 如图 5-89 所示，右击“销售部员工”选项，在弹出的快捷菜单中选择“刷新”命令，可以看到凡

是用户账户部门属性是“销售部”的，自动被查找出来。

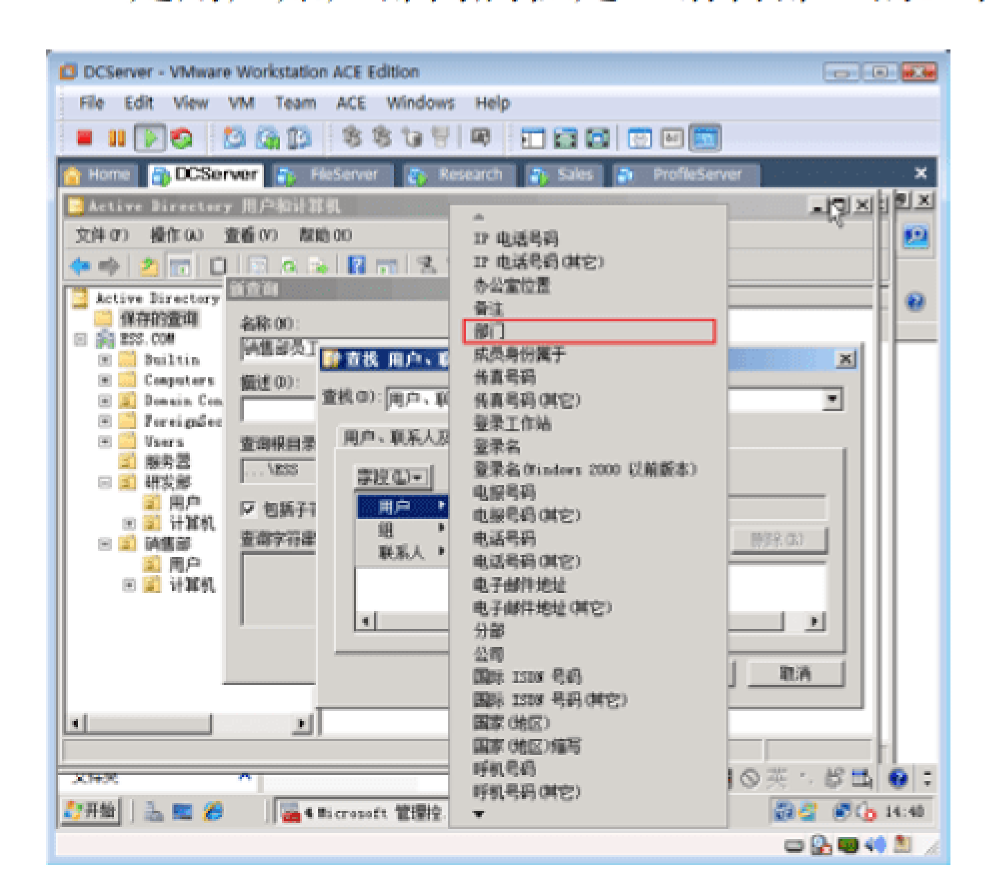


图 5-84 指定查询条件

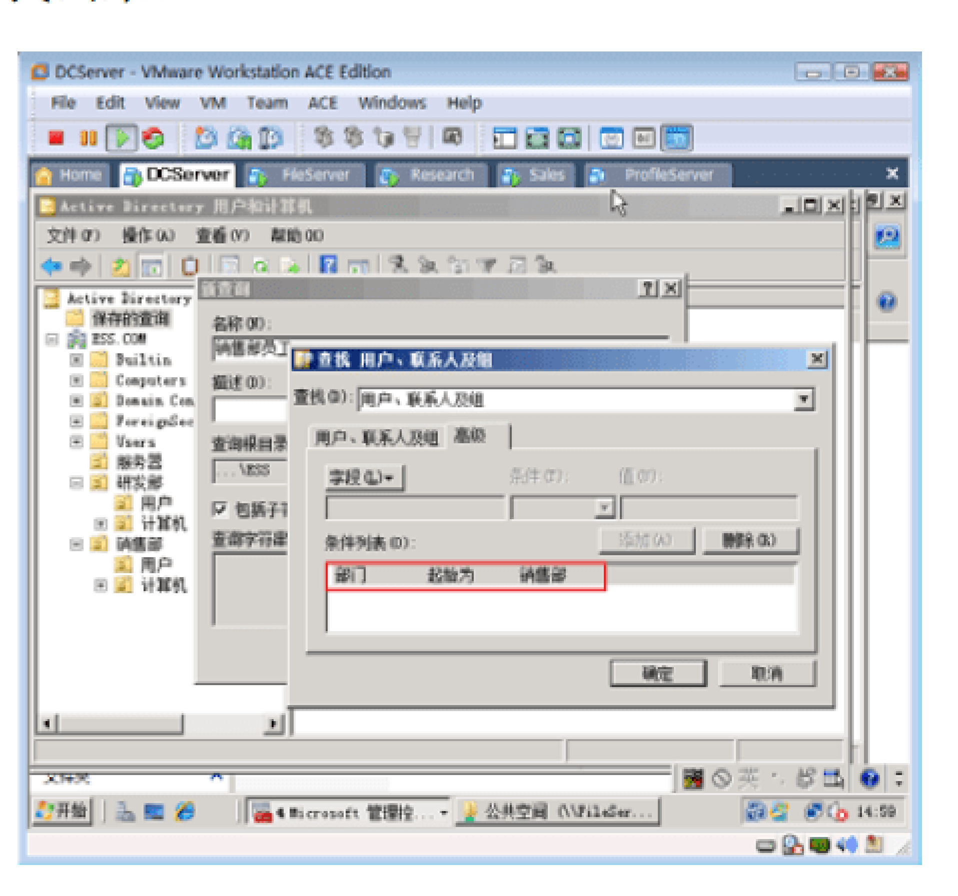


图 5-85 指定查询条件的值

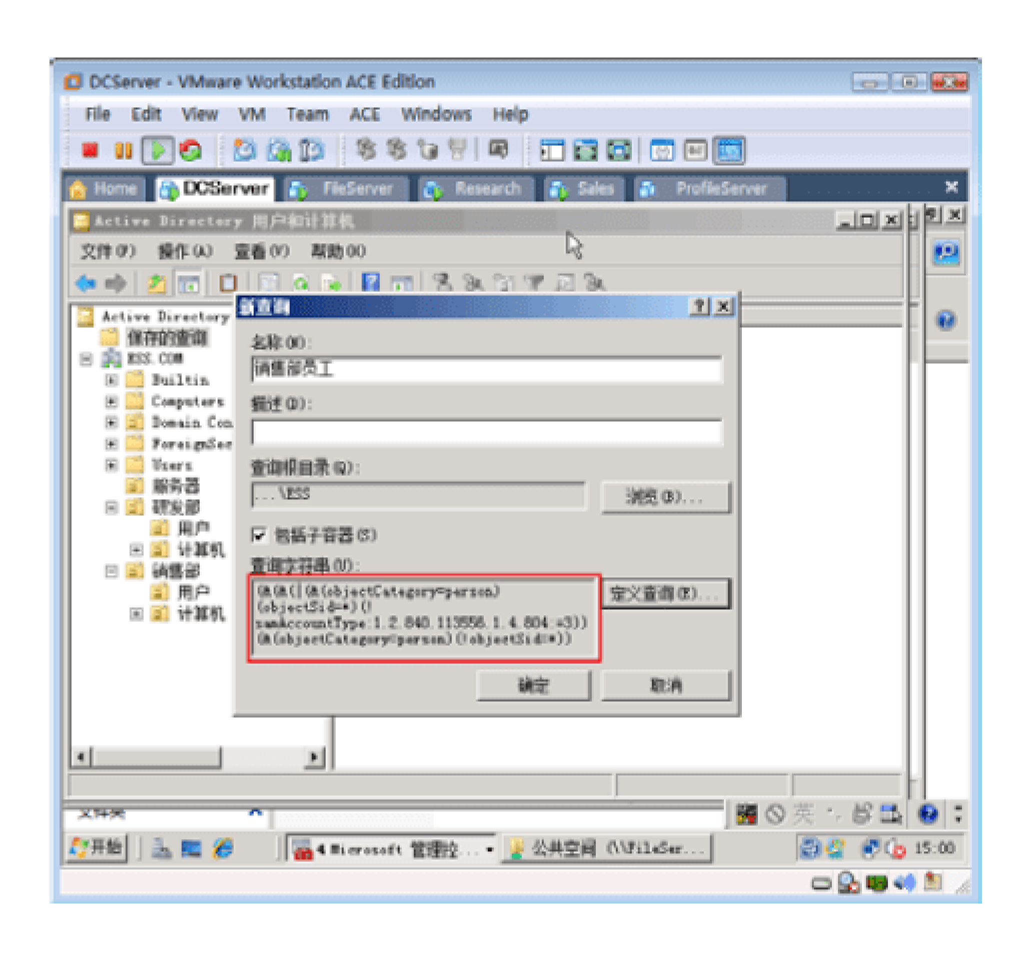


图 5-86 自动生成查询语句

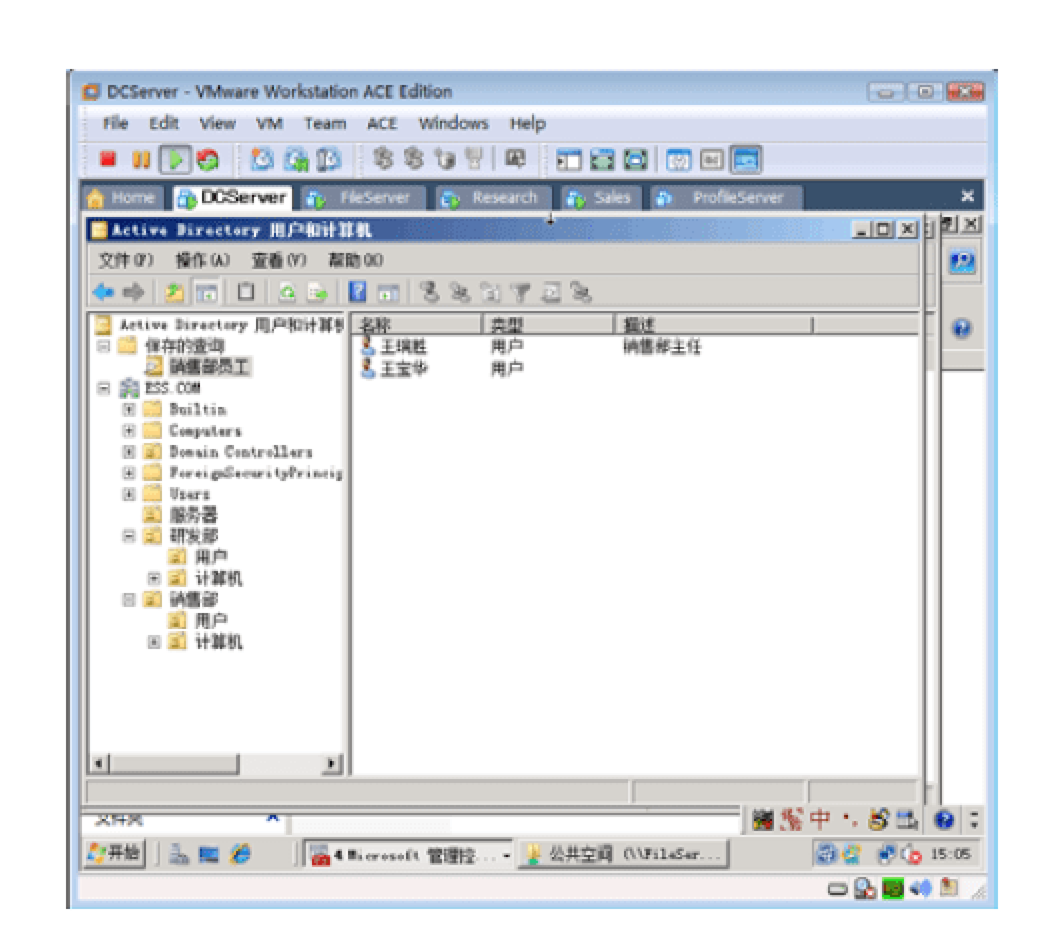


图 5-87 查看查询出来的用户

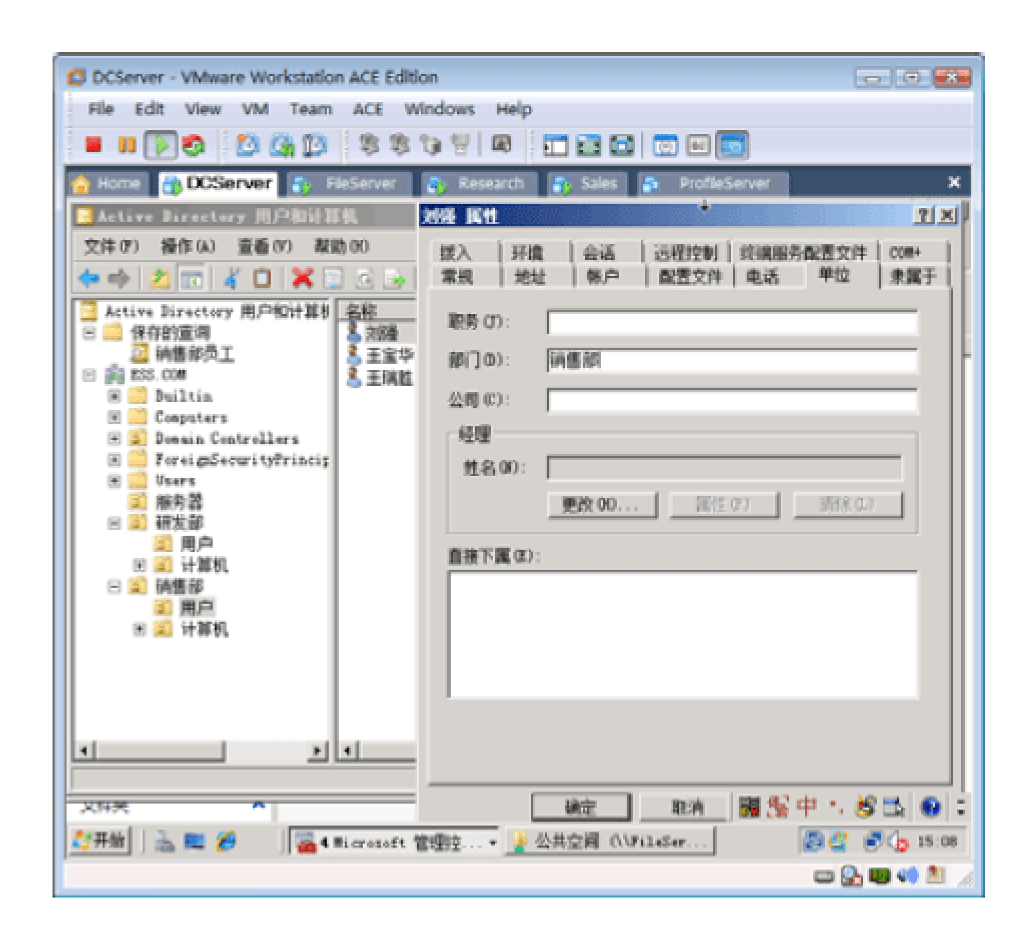


图 5-88 将用户指定到销售部

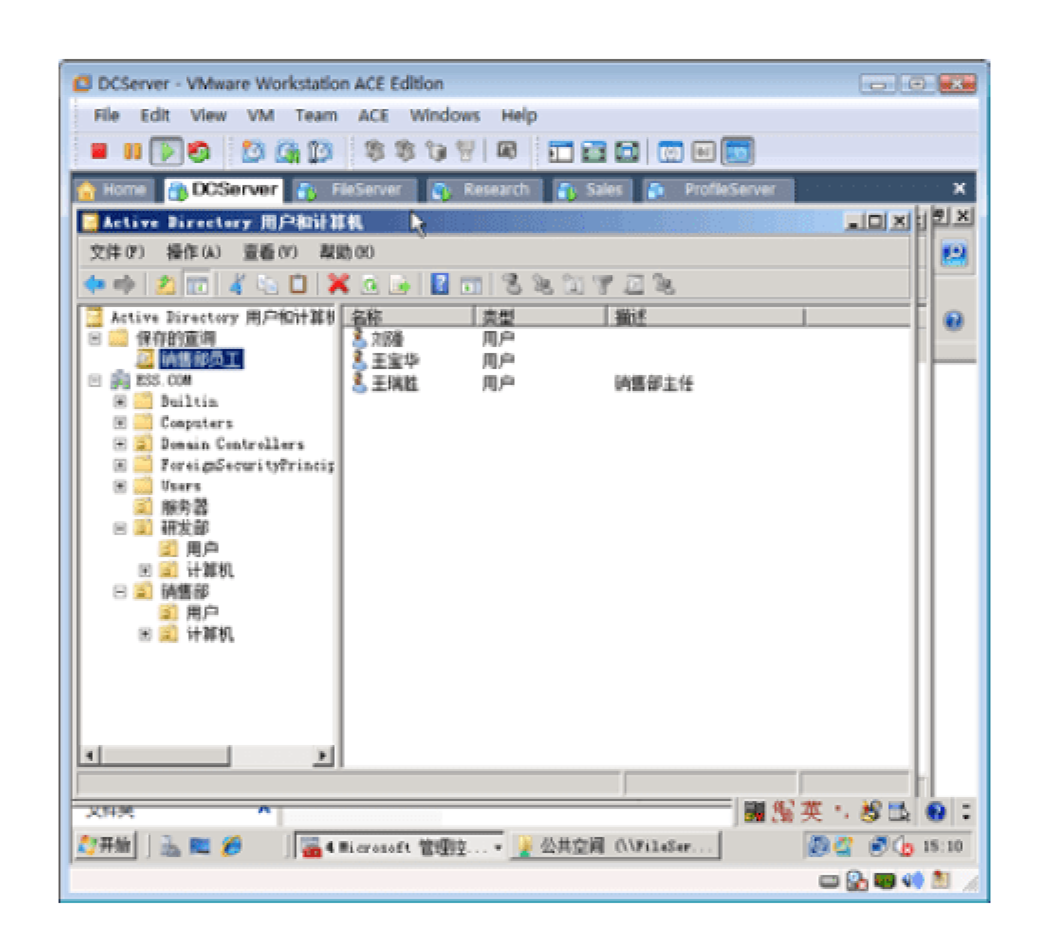


图 5-89 查看销售部的用户

5.5 用户配置文件

用户配置文件是使计算机符合所需的外观和工作方式的设置的集合，其中包括桌面背景、屏幕保护程序、指针首选项、声音设置及其他功能的设置。用户配置文件可以确保只要登录到 Windows 便会使用个人首选项。

用户配置文件与用于登录到 Windows 的用户账户不同。每个用户账户至少有一个与其关联的用户配置文件。

每一个用户配置文件都以 Default 的副本开始，这是存储在运行 Windows Server 2008 操作系统的所有计算机上的默认用户配置文件。Default 中的 NTuser.dat 文件包含 Windows Server 2008 家族配置设置。“公共”配置文件的更改会影响到所有用户。

5.5.1 查看用户配置文件和公共配置文件

下面介绍如何查看用户“Default”配置文件、“公共”文件夹以及 Research 计算机上的用户的配置文件。

1. 任务

- 查看 Default 配置文件。
- 查看配置文件结构。
- 了解公共配置文件的作用。

2. 步骤

① Windows Server 2008 的用户配置文件默认在 c:\用户\目录下。

② 如图 5-90 所示，打开“c:\用户”目录，单击“组织”，在其下拉菜单中选择“文件夹和搜索选项”命令。

③ 如图 5-91 所示，在“文件夹选项”对话框中，切换到“查看”选项卡，选择“显示隐藏的文件和文件夹”单选按钮，单击“确定”按钮。

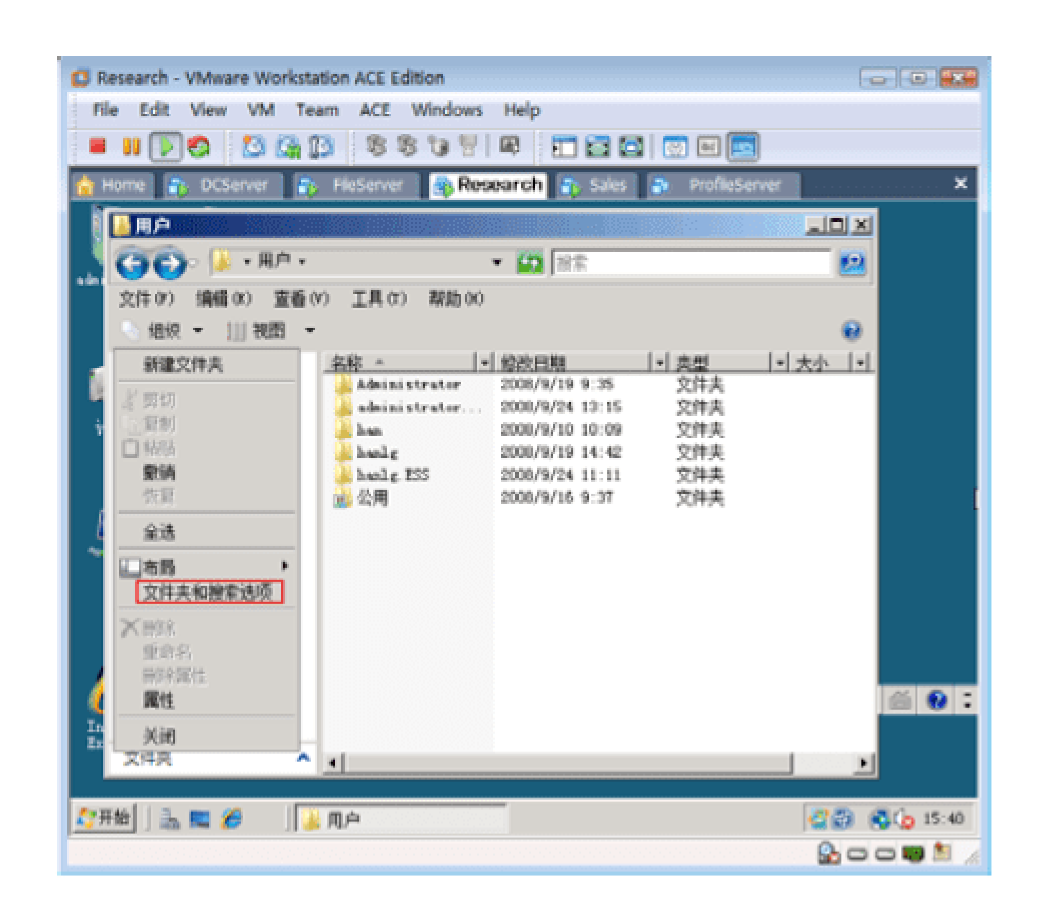


图 5-90 打开文件夹选项设置

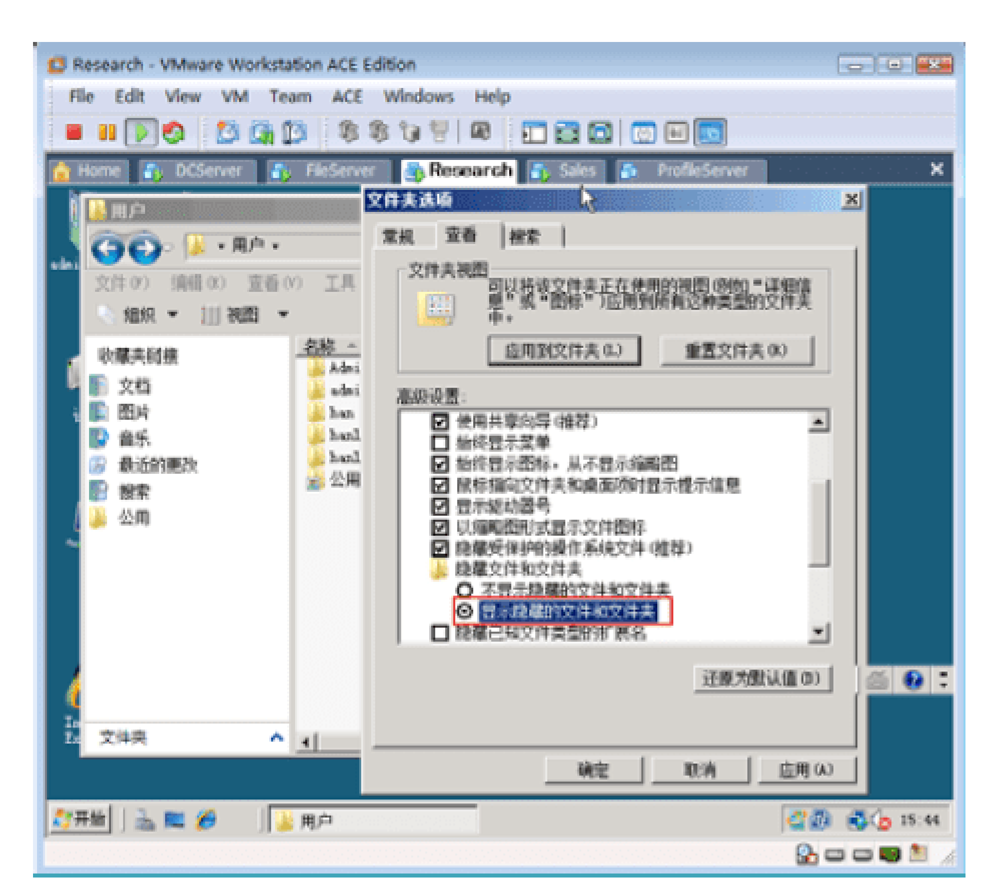


图 5-91 显示隐藏的文件和文件夹

④ 如图 5-92 所示，此时能够显示隐藏的 Default 文件夹。

⑤ 用户配置文件文件夹包含各种项目，包括桌面和“开始”菜单。图 5-93 列出了每个用户配置文件中的文件夹。

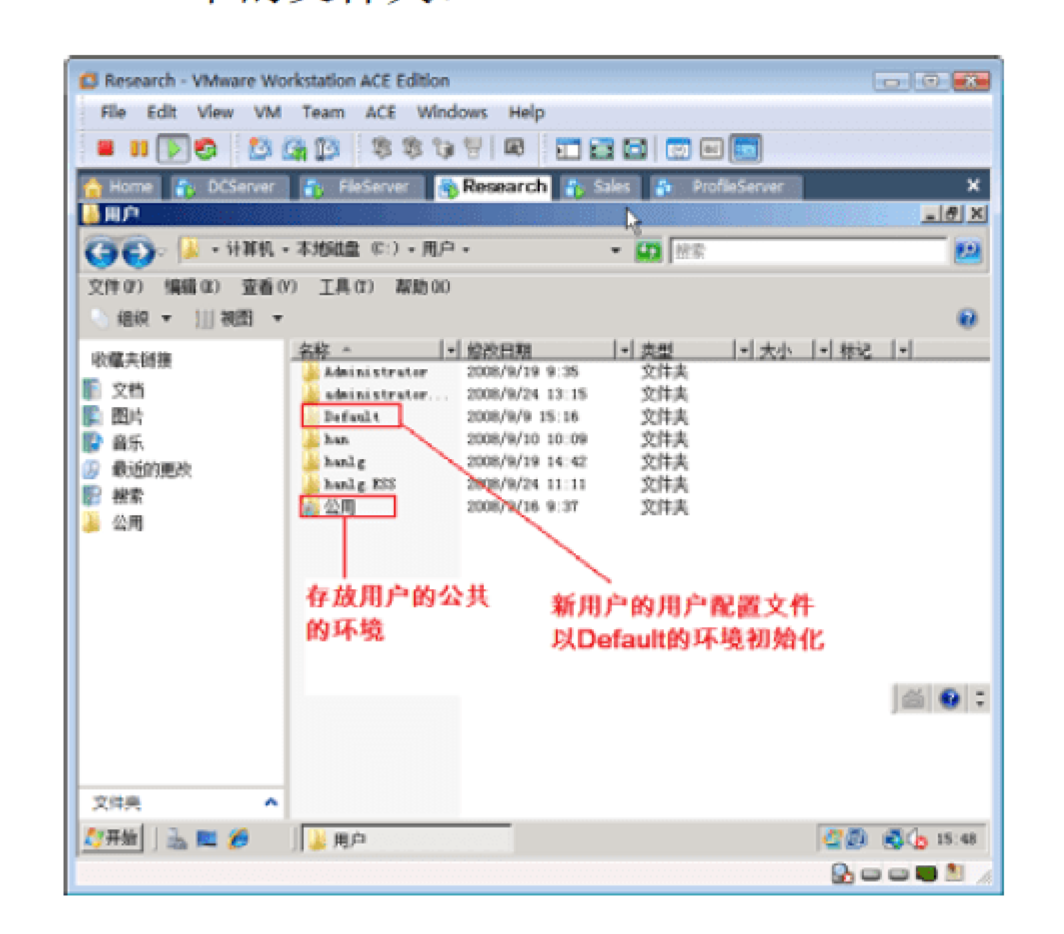


图 5-92 默认配置文件

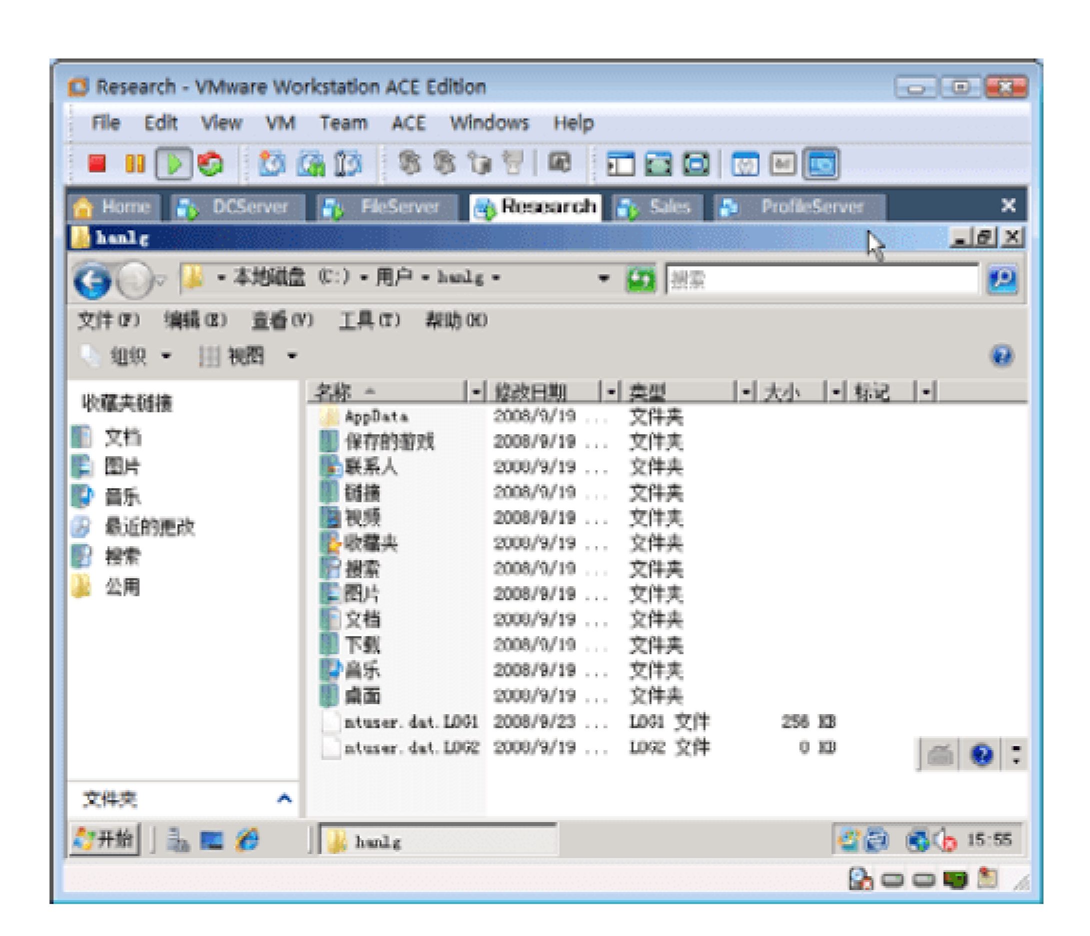


图 5-93 配置文件的结构



提示：每个用户配置文件还使用包含在“公用”文件夹中的公用程序组。比如，打算让任何使用这台计算机的用户桌面上都有访问微软站点的快捷方式，则可以在“公用”文件夹中的“公用桌面”中创建一个快捷方式。

⑥ 如图 5-94 所示，打开“公用”文件夹中的“公用桌面”，右击空白处，在弹出的快捷菜单中选择“新建”→“快捷方式”命令。

⑦ 如图 5-95 所示，在出现的“创建快捷方式”对话框中，输入 http://www.microsoft.com/china，单击“下一步”按钮。

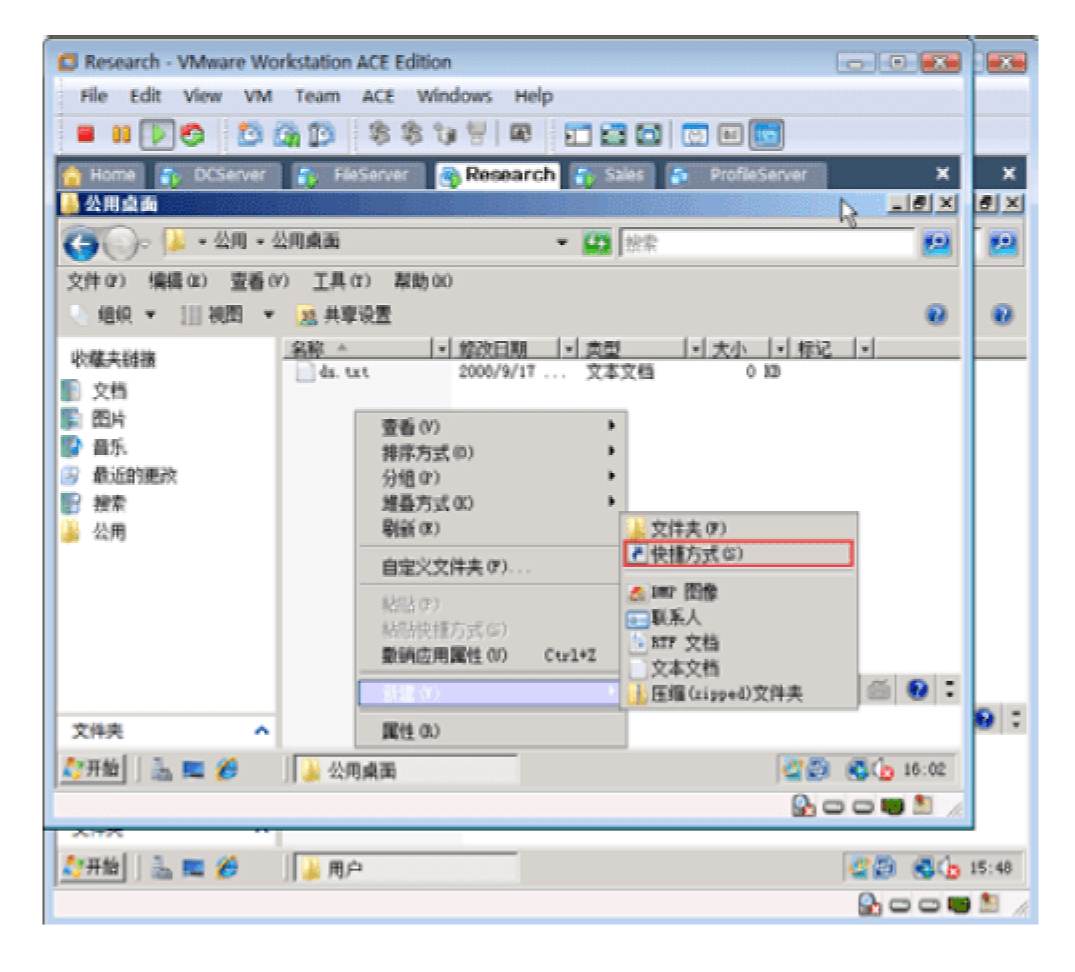




图 5-94 创建快捷方式

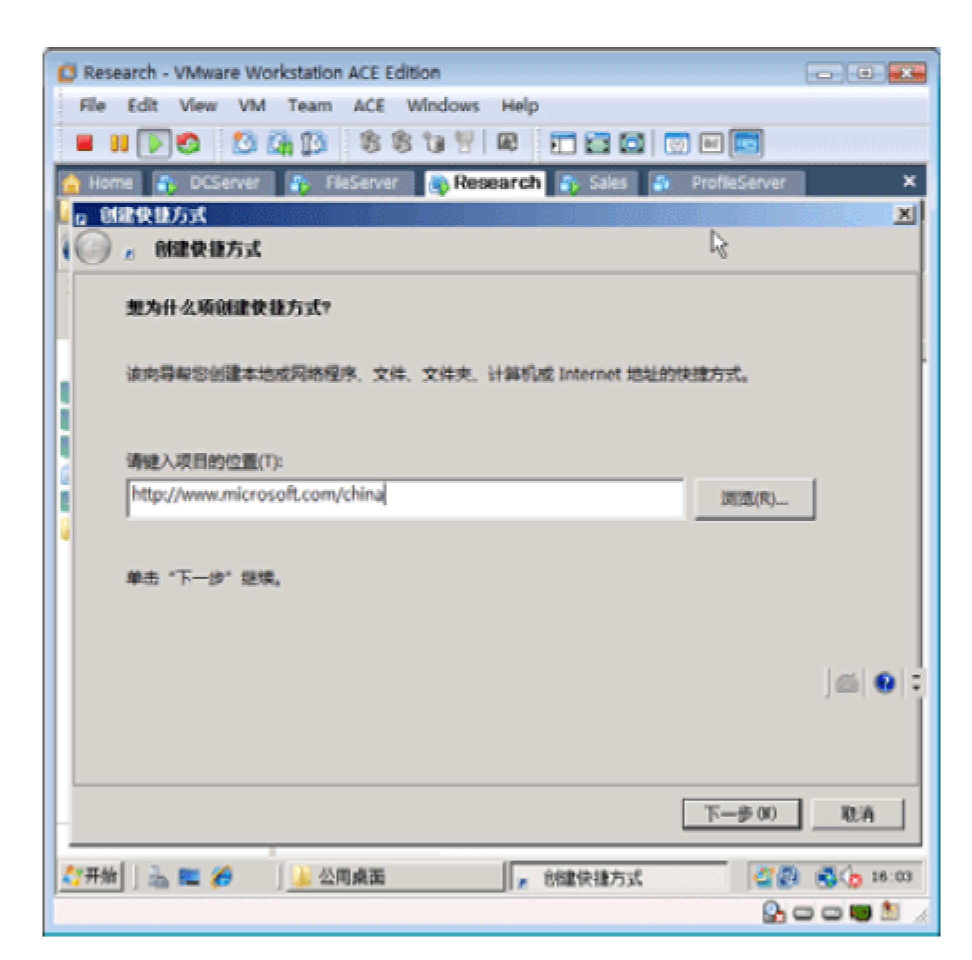


图 5-95 输入网址

⑧ 如图 5-96 所示，在出现的对话框中，输入快捷方式名称“微软中文站点”，单击“完成”按钮。

⑨ 如图 5-97 所示，显示自己的桌面，发现在“公用桌面”中创建的快捷方式出现在自己的桌面上。

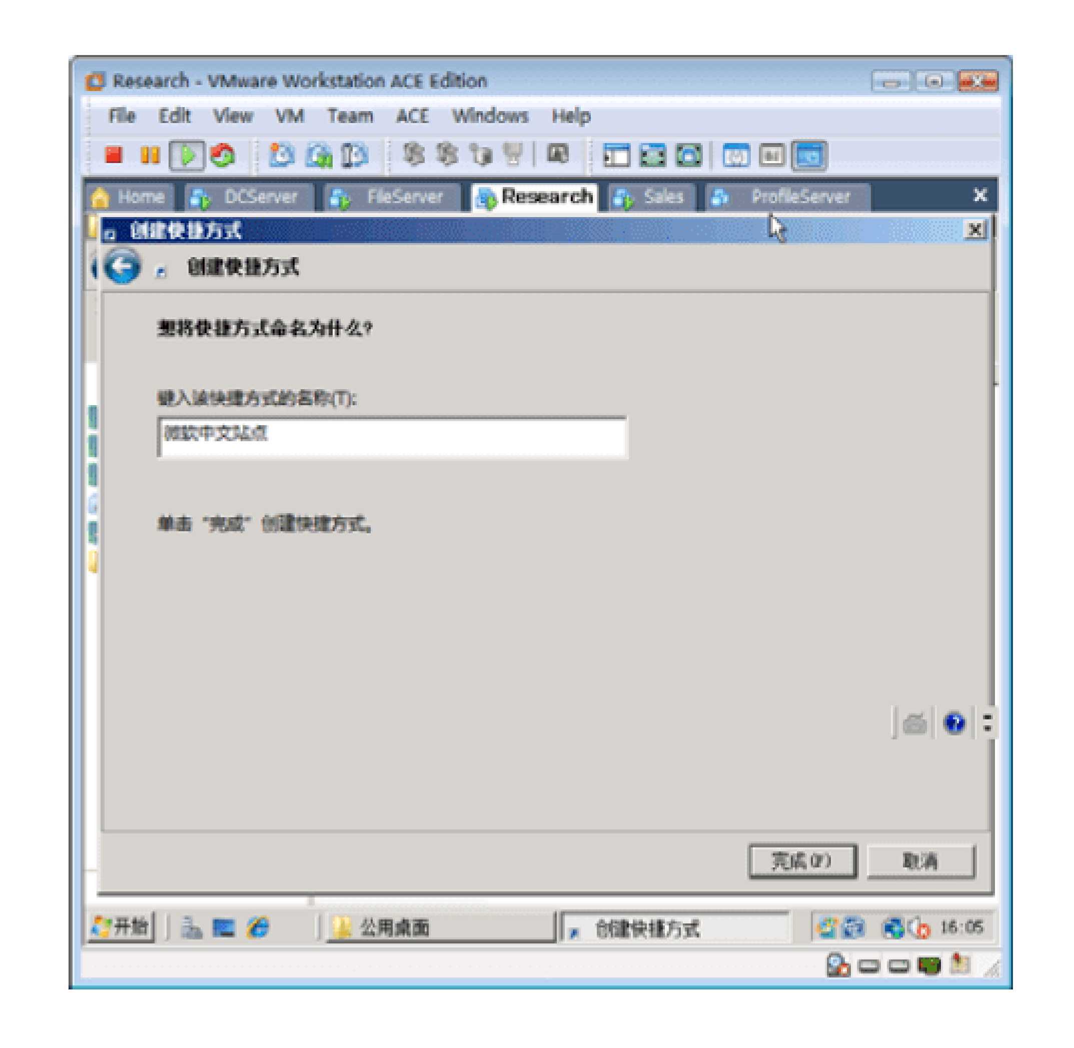


图 5-96　输入快捷方式的名称

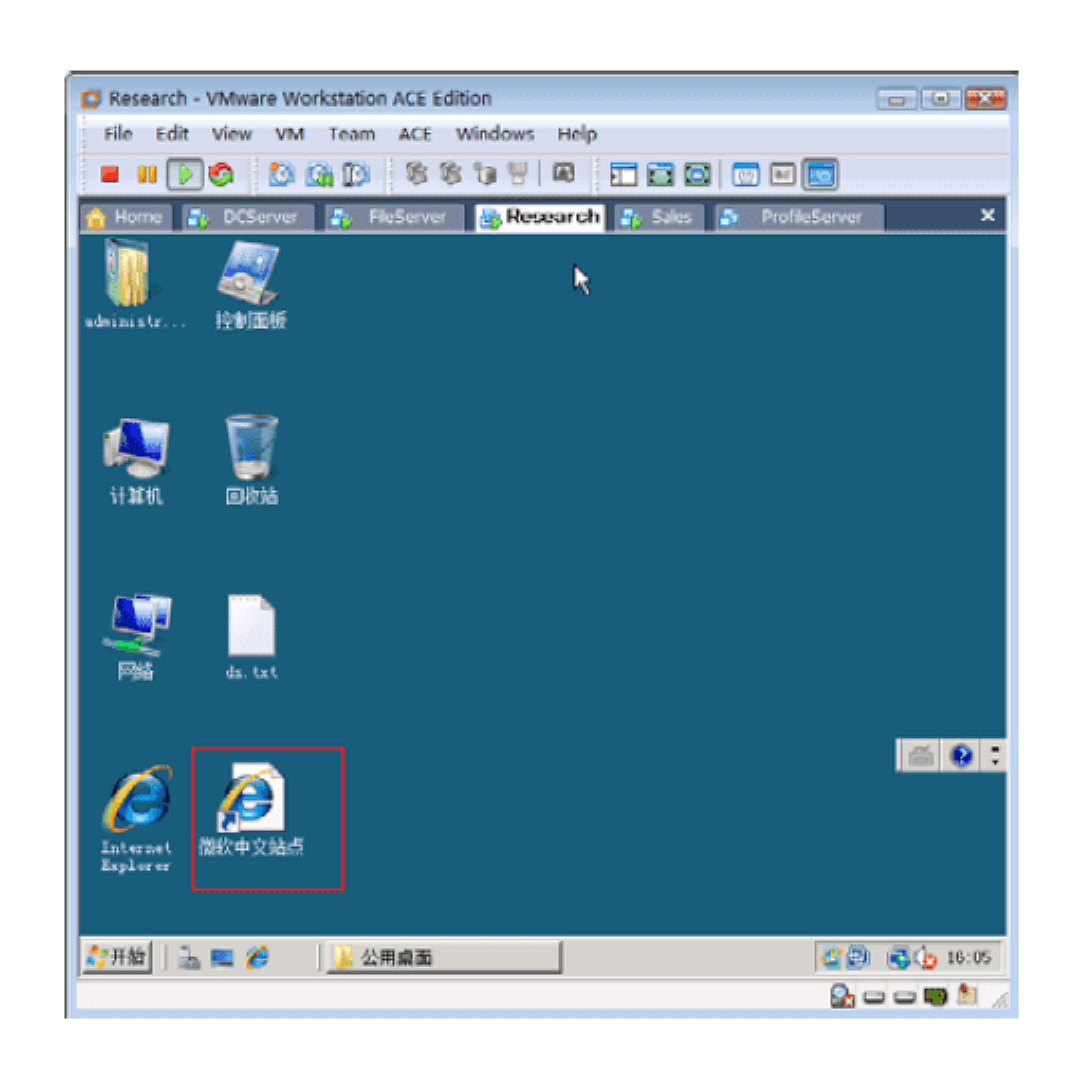


图 5-97　当前用户桌面出现快捷方式

5.5.2　用户配置文件的类型

1. 本地用户配置文件

当一个用户第一次登录到一台计算机上时，创建的用户配置文件就是本地用户配置文件。一台计算机上可以有多个本地用户配置文件，分别对应于每一个曾经登录过该计算机的用户。域用户的配置文件夹的名字的形式为“用户名.域名”，而本地用户的配置文件的名字是直接以用户命名的。用户配置文件不能直接被编辑。要想修改配置文件的内容需要以该用户登录，然后手动修改用户的工作环境如桌面、“开始”菜单、鼠标等，系统会自动地将修改后的配置保存到用户配置文件中。

2. 漫游用户配置文件

该文件只适用于域用户，域用户才有可能在不同的计算机上登录。

当一个用户需要经常在其他计算机上登录，并且每次都希望使用相同的工作环境时就需要使用漫游用户配置文件。该配置文件被保存在网络中的某台服务器上，并且当用户更改了其工作环境后，新的设置也将自动保存到服务器上的配置文件中，以保证其在任何地点登录都能使用相同的新的工作环境。所有的域用户账户默认使用的是该类型的用户配置文件。该文件是在用户第一次登录时由系统自动创建的。

3. 强制性用户配置文件

强制性用户配置文件不保存用户对工作环境的修改，当用户更改了工作环境参数之后退出登录再重新登录时，工作环境又恢复到强制用户配置文件中所设定的状态。当需要一个统一的工作环境时该文件就十分有用。该文件由管理员控制，可以是本地的也可以是漫游的用户配置文件，通常将强制性用户配置文件保存在某台服务器上，这样不管用户从哪台计算机上登录都将得到一个相同且不能更改的工作环境。因此强制性用户配置文件有时也被称为强制性漫游用户配置文件。

5.5.3 创建漫游用户配置文件

假设“刘强”来使用漫游用户配置文件，并且将这个用户的漫游用户配置文件存储在服务器 FileServer 上的共享文夹 Profiles 中。

1. 任务

- 为漫游式配置文件创建并共享文件夹。
- 为用户指定一个空的漫游用户配置文件。

2. 步骤

① 如图 5-98 所示，以域管理员的身份登录 FileServer 服务器，创建一个文件夹 profiles，右击该文件夹，在弹出的快捷菜单中选择“共享”命令。

② 在出现的“选择要与其共享的网络上的用户”对话框中，选择“查找”选项。

③ 在出现的“选择用户组”对话框中，输入 Domain Users，单击“检查姓名”，设置共享权限为 Domain Users，为“参与者”，单击“共享”按钮，单击“完成”按钮。

④ 如图 5-99 所示，在 DCServer 上，打开“Active Directory 用户和计算机”窗口，双击“刘强”用户账户，在用户属性对话框中，切换到“配置文件”选项卡，输入 \\fileServer\profiles\%username%。


注意：其中，%username%是参数，自动以用户账户登录名替换。

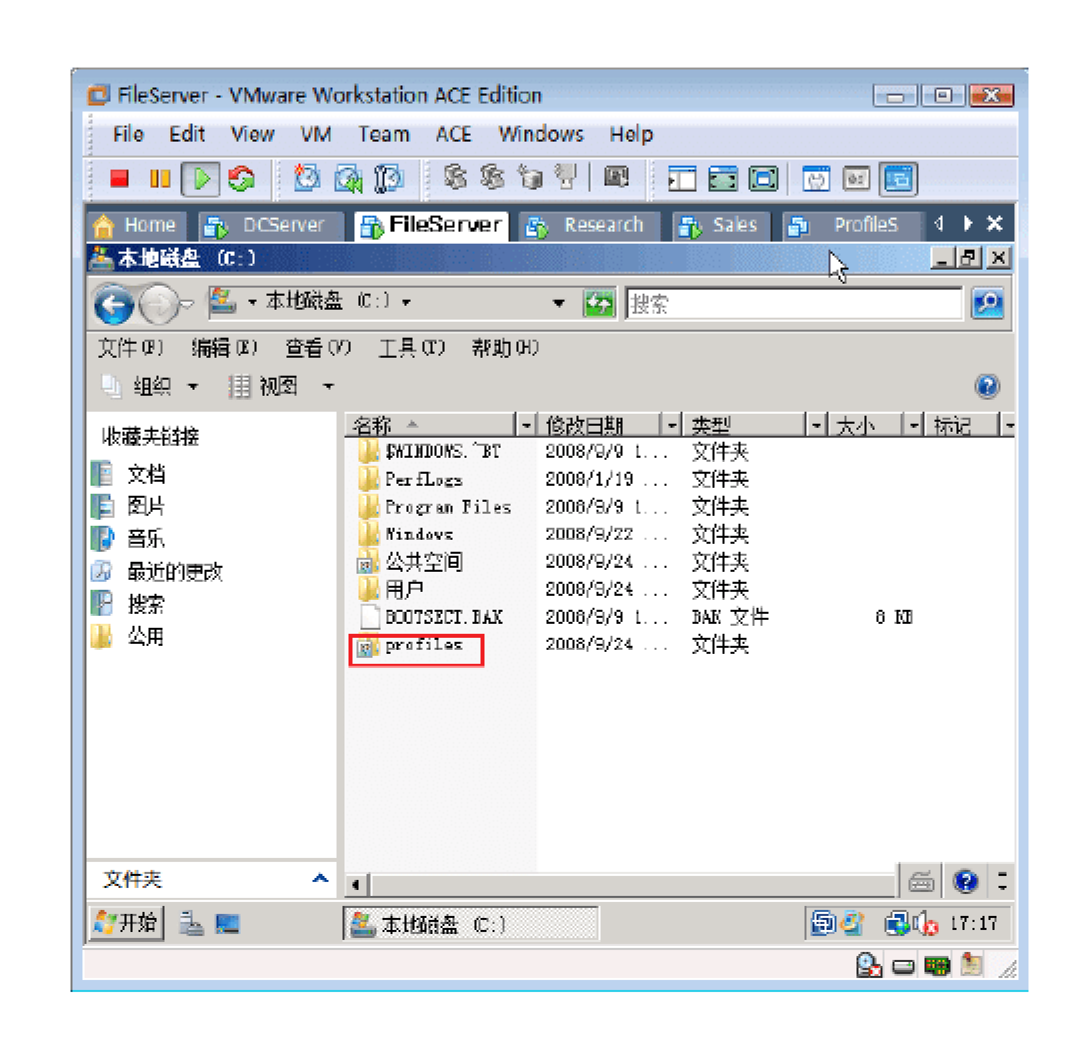


图 5-98 为漫游式配置文件共享文件夹

图 5-99 为域用户指定配置路径

⑤ 使用“刘强”账户登录 Research 计算机，将计算机的桌面换成一个“刘强”文件夹中的图片，将开始菜单改为经典模式，在桌面上创建一个记事本文件“刘强 Research.txt”，如图 5-100 所示，注销计算机。

⑥ 使用“刘强”账户在 Sales 上登录，可以看到开始菜单是经典模式，桌面上有“刘强 Research.txt”文件。



注意：

- 该桌面背景使用的图片最好位于用户配置文件夹中的目录中，比如"我的文档"中的"图片"文件夹中；否则换一台计算机登录没有办法引用该图片。
- 必须在 Research 计算机上注销，因为在注销的时候才会把更改后的用户的配置文件保存到服务器 FileServer 上。
- 用户的环境包括鼠标指针左右手习惯、桌面背景图片、映射的网络驱动器、连接的网络打印机等设置。通过漫游式用户配置文件使用户的工作环境只与用户账户有关，而与使用的计算机无关。

注意：桌面上的"微软中文站点"没有在 Sales 的计算机桌面上出现，这是因为这个快捷方式位于 Research 计算机"公用"文件夹的"公用桌面"文件夹中，如图 5-101 所示。

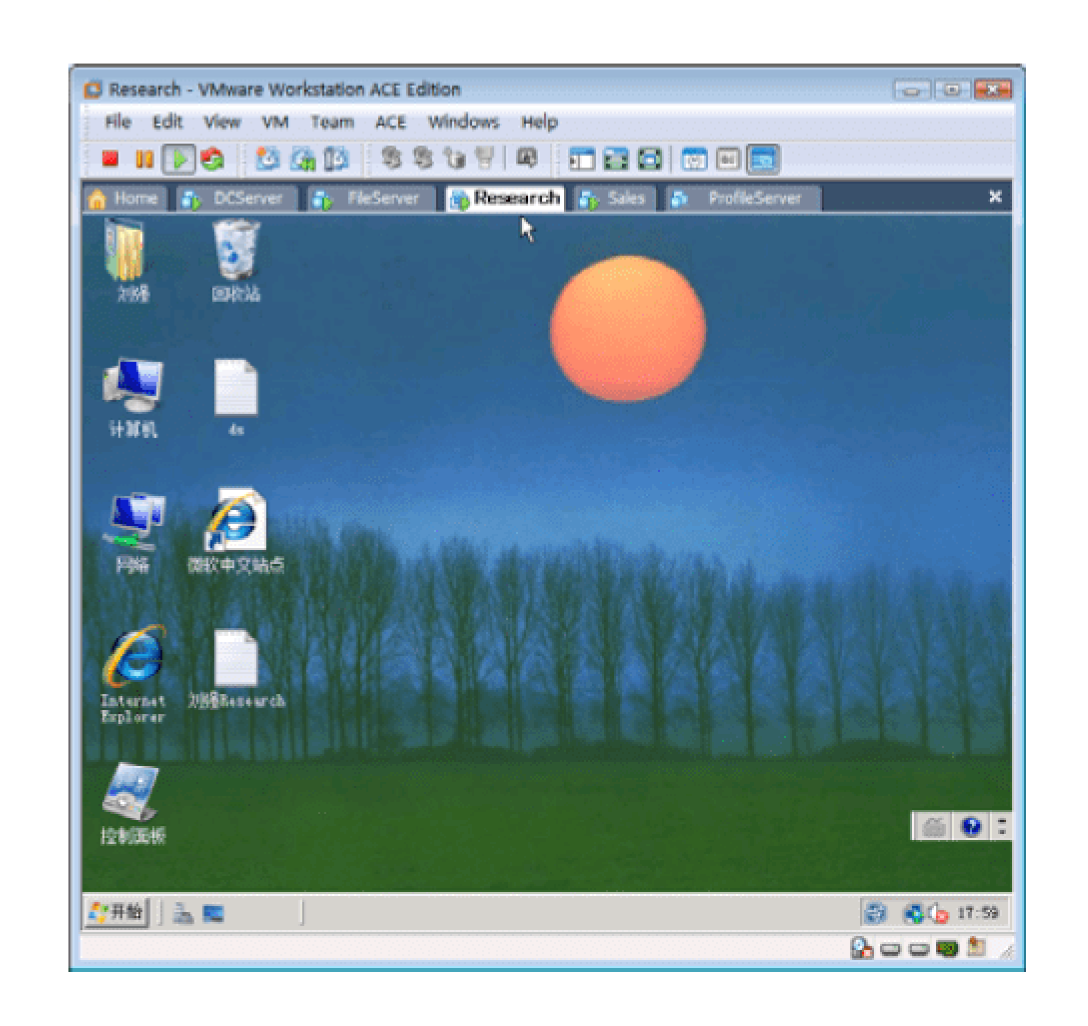


图 5-100 第一次登录后更改桌面环境

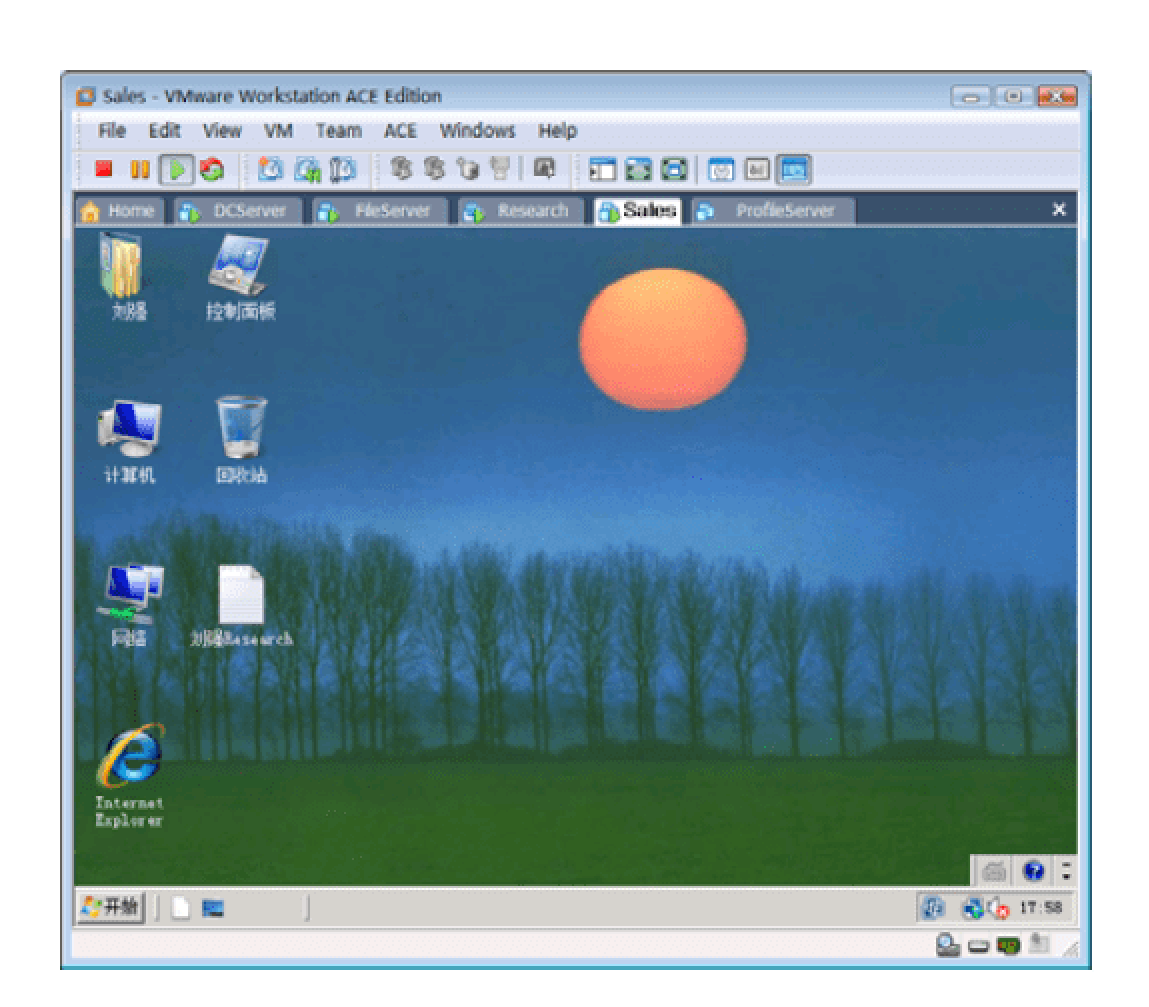


图 5-101 换一台计算机登录环境漫游

5.5.4 漫游配置文件应用过程

漫游用户配置文件的用户在登录域时，其计算机会读取存储在服务器端的漫游用户配置文件，以便根据该配置文件来决定用户的桌面设置。而用户注销时，用户的桌面设置会被同时保存在漫游用户配置文件与本地用户配置文件内。

如果用户在登录域时，因故无法访问服务器内的漫游用户配置文件，例如网络断线、权限不够，则会出现如图 5-102 所示的警告信息。

- 如果该用户是第一次登录这台计算机，则因为该计算机内当前还没有该用户的本地用户配置文件，因此系统会以 Default 配置文件的内容设置用户环境。当用户注销时，其桌面设置既不会被存储到服务器上的漫游用户配置文件内，也不会被存储在本地用户配置文件内。
- 如果该用户以前曾经登录过这台计算机，则将使用他在该计算机内的本地用户配置文件。当用户注销时，其桌面设置并不会被存储到服务器上的漫游用户配置文件内，只会被存储到本地用户配置文件内。而用户下一次登录域时，即使网络断线、权限不够等问题已经解决，也就是已经可以正常访问服务器上的漫游用户配置文件，但是由于本地用户配置文件的数据比较新，因此仍然会

使用本地用户配置文件。不过注销时，就可以正常地将桌面设置存储到漫游用户配置文件内了。

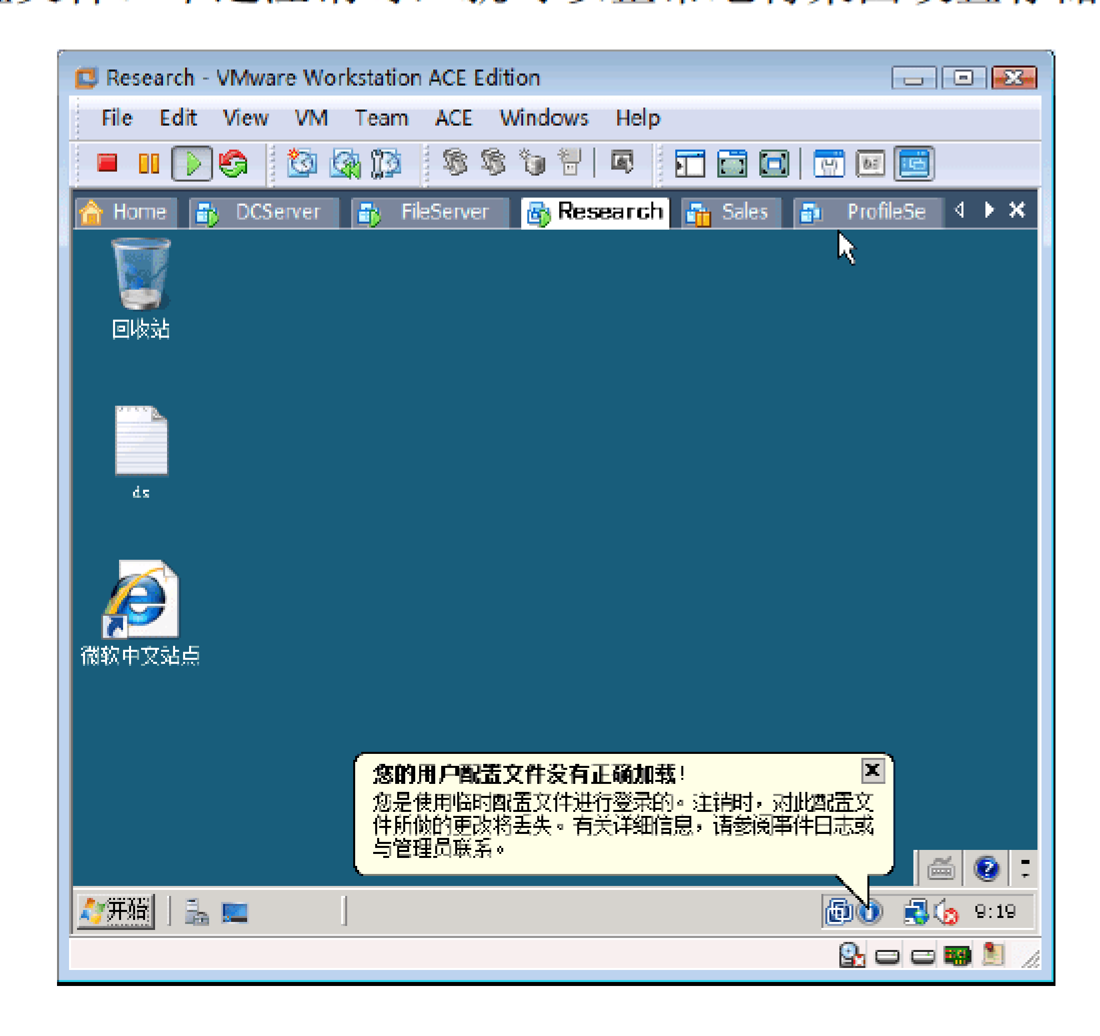


图 5-102　用户配置文件没有正确加载

5.6　在活动目录中使用组

5.6.1　组的类型

如图 5-103 所示，活动目录中组有两种类型：安全组和通讯组。

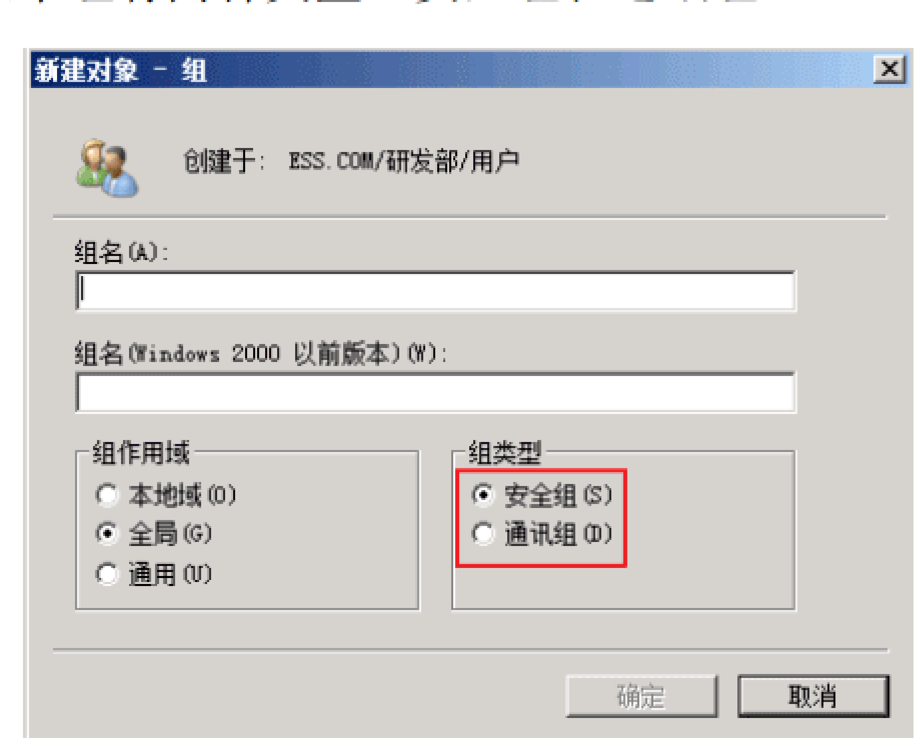


图 5-103　组的类型

1. 安全组

安全组有安全标识(SID)，能够给其授权用户访问本地资源或网络资源。既能授权访问资源，也可以利用其群发电子邮件。

2. 通讯组

通迅组没有安全标识(SID)，不能授权其访问资源，只能用来群发电子邮件。如果你安装了微软的邮件系统 Exchange，可以创建一些专门群发电子邮件的通讯组。这样你就可以在收件人处输入通讯组的电子邮

件地址，邮件服务器会读取通迅组的成员，将电子邮件发送到该组的所有成员。

5.6.2 组的作用域

活动目录中组按照能够授权的范围，分为本地域组、全局组和通用组，如图 5-104 所示。下面将分别介绍创建这几类组的目的。

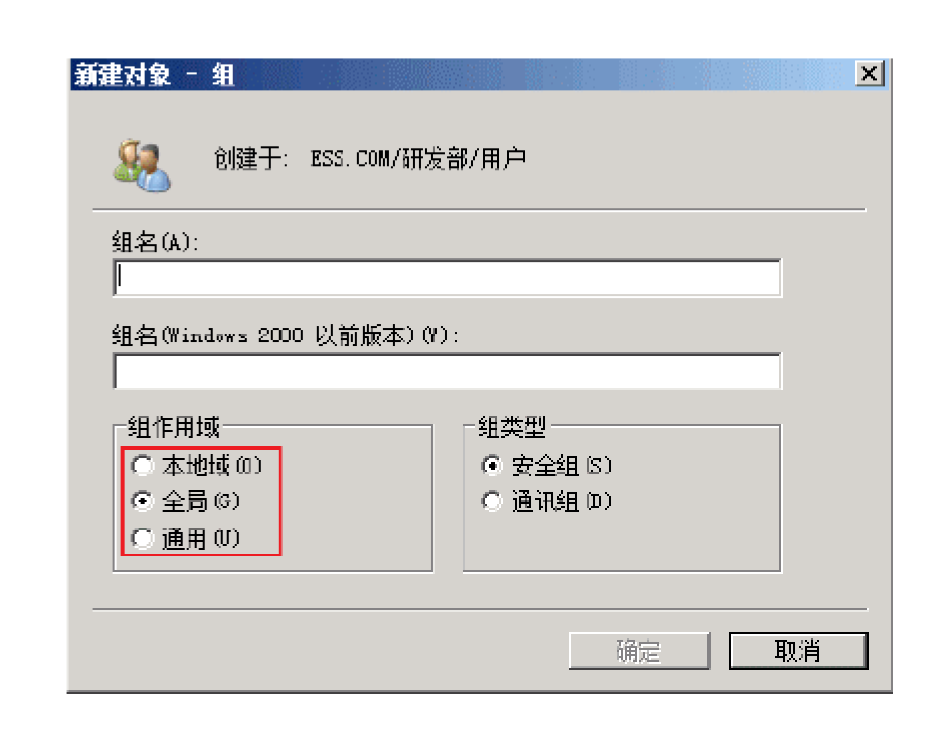


图 5-104 组的作用域

1. 本地域组

本地域组代表的是对某种资源的访问权限。

创建本地域组的目的是针对某种资源的访问情况而创建的。比如在网络上有一个激光打印机，针对该打印机的使用情况，可以创建一个“激光打印机使用者”本地域组；然后授权该组使用该打印机。以后哪个用户或全局组需要使用打印机，可直接将用户或组添加到“激光打印机使用者”，就等于授权使用打印机了。可以针对 FileServe 服务器上“公共空间”文件夹创建一个“公共空间访问者”本地域组，然后授予该“公共空间访问者”对“公共空间”的读/写权限。

自己创建的本地域组，可以在授权访问本域计算机上的资源，它代表的是访问资源的权限；其成员可以是本域的用户、组或其他域的用户组；只能授权其访问本域资源，其他域中的资源不能授权其访问。

2. 全局组

全局组代表的是同类用户身份的用户账户。

创建全局组是为了合并工作职责相似的用户账户。比如为了合并研发部的员工，可以创建一个“研发部员工”全局组；为了合并销售部的员工，可以创建一个“销售部员工”的全局组；当然如果想合并部门经理的用户账户，你可以创建“研发部经理”全局组、“销售部经理”全局组。

只能将本域的用户和组添加到全局组。在多域环境中不能合并其他域中的用户。

能够授权访问整个域中的资源，在多域环境中其他域的资源也能授权其访问。

3. 通用组

和全局组的作用一样，目的是根据用户的职责合并用户。

与全局组不同的是，在多域环境中它能够合并其他域中的域用户账户，比如可以把两个域中的经理账户添加到一个通用组。

在多域环境中，可以在任何域中为其授权。

5.6.3 在域环境中使用组的策略

将用户账户(User Acounts)添加到全局组(Global Group)，将用户账户合并。

将为本地域组(Domain Local Group)授权(Permission)对某资源的访问。

授权的过程就变为将全局组(Global Group)添加到本地域组(Domain Local Group)的过程。

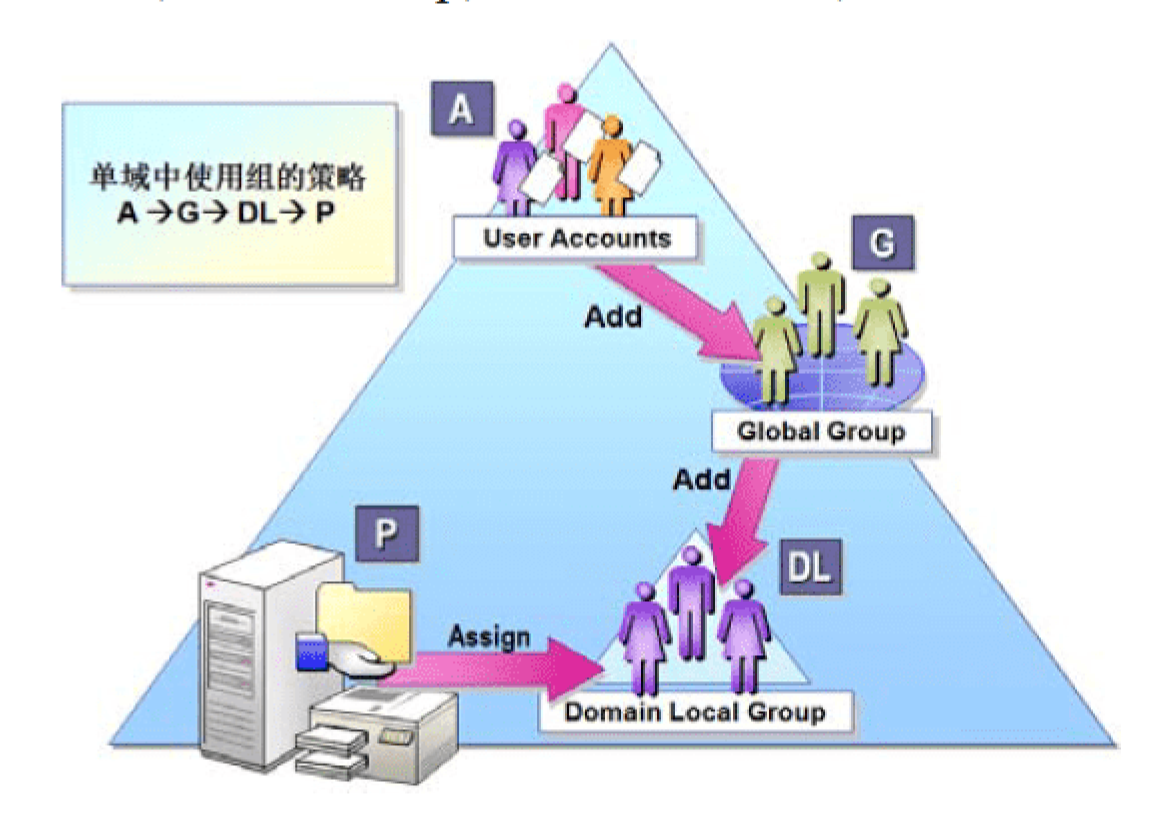


图 5-105　使用组的策略

总结

在单域中使用组的策略是 A→G→DL→P 策略，如图 5-105 所示。如果域中的用户账户不多，则可以直接授权用户或全局组访问某资源。如果用户账户较多，最好使用推荐的 A→G→DL→P 策略，调理清晰。

在多域环境中使用组的策略是 A→G→U→DL→P 策略。U 代表(Universal Group)，即将用户账户添加到本域的全局组，然后将各个域的全局组添加到通用组，将通用组添加到本地域组，为本地组授权。

5.6.4　内置的本地域组

在 Windows Server 2008 域控制器的活动目录中，系统内置了一些本地域组，这些组本身已经被赋予一些权限与权利，以便让其具备管理整个域或活动目录的能力。只要将用户或组账户加入到这些内置的本地域组中，这些账户也将具有相同的权利与权限。

这些内置的本地域组位于活动目录的 Builtin 容器内，如图 5-106 所示。下面列出几个较常用的本地域组。

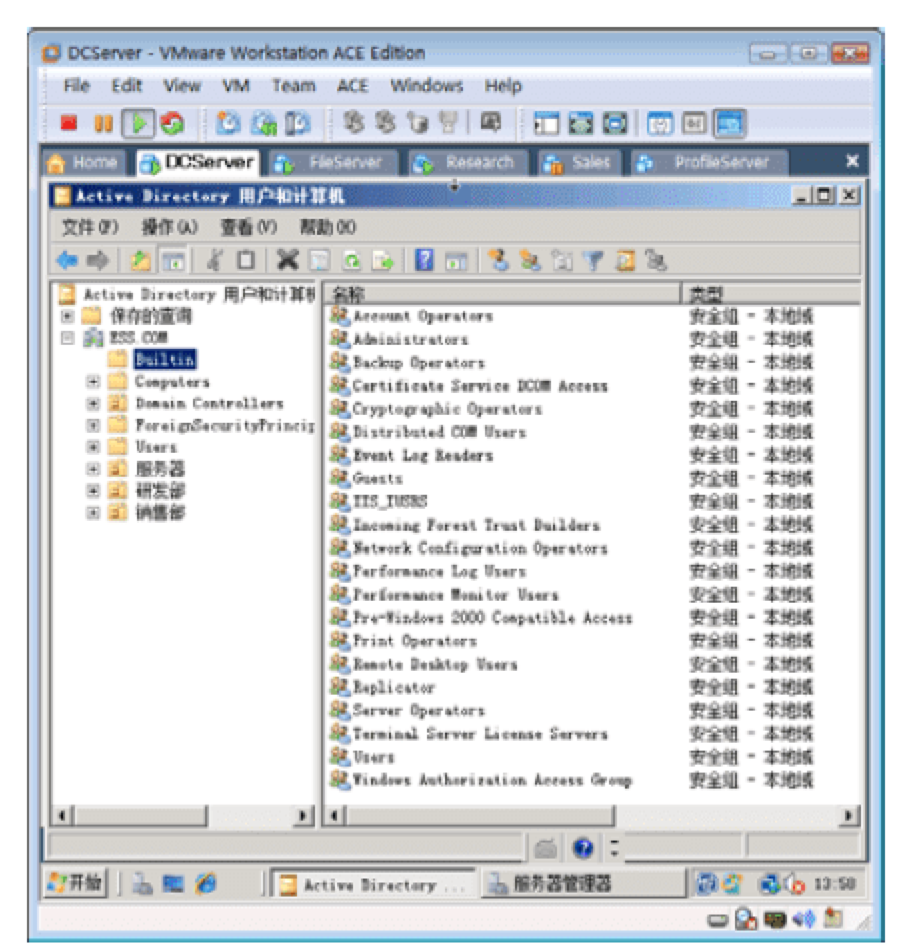


图 5-106　内置的本地域组

- Account Operators 成员可以管理域用户和组账户，系统默认他们可以在任何一个容器与组织单元内(但是 Builtin 容器与 Domain Controller 组织单位除外)新建、删除、更改用户账户、组账户、计算机账户。但他们无法更改或删除 Administrators 与 Domain Admins 组的成员。
- Administrators：属于该 Administrators 本地域组中的用户都具备系统管理员的权限，他们拥有对整个域控制器最大的控制权，可以执行整个活动目录的管理任务。内置的管理员账户 Administrator 就是该本地域组的成员，而且无法将其从该组中删除。该 Administrators 组默认的成员包含 Administrator、Domain Admins 全局组、Enterprice Admins 全局组等。

- Backup Operators：Backup Operators 本地域组的成员可以备份与还原域控制器中的文件夹与文件。Backup Operators 的成员还可以关闭域控制器。
- Guests：该本地域组是供没有用户账户，但是需要访问资源的用户使用。该组的成员无法永久改变其桌面的工作环境。该组默认的成员为用户账户 Guest 与全局组 Domain Guest。
- Network Configuration Operators：该组内的用户，可以在域控制器上执行一般的网络设置操作，例如，更改 IP 地址，但是不可以安装/删除驱动程序与服务，也不可以执行与网络服务器设置有关的任务，例如，对 DNS 服务器、DHCP 服务器进行设置。
- Pre-Windows 2000 Compatible Access：该组主要是为了与 Windows NT 4.0 计算机兼容。其成员可以读取 Windows Server 2008 域中的所有用户与组账户。默认的成员为特殊组 Authenticated Users。只有在用户所使用的计算机是 Windows NT 4.0 或更旧的系统时，才将用户加入到该组中。
- Print Operators 成员可以创建、停止或管理在域控制器上的共享打印机，也可以关闭计算机。
- Remote Desktop Users：此组中的成员被授予远程登录的权限，比如使用其他计算机通过远程桌面或终端服务连接到域控制器登录。
- Server Operators 成员可以创建、管理、删除域控制器上共享文件夹与打印机，备份与还原域控制器内的文件，锁定与解开域控制器，将域控制器上的硬盘格式化，更改域控制器的系统时间，关闭域控制器等。
- Users：该 Users 本地域组的成员拥有一些基本的权限，例如运行程序，但是他们不能修改操作系统的设置，不能更改其他用户的数据，不能关闭服务器级的计算机。该组默认的成员为 Domain Users 全局组。

5.6.5 内置的全局组

当创建一个域时，系统会在活动目录中创建一些内置的全局组。这些全局组本身并没有任何权限与权利，但是可以通过将其加入到具备权利或权限的本地域组，或者直接为全局组指派权限或权利。

这些内置的全局组位于 Users 容器内。下面列出几个较常见的全局组，如图 5-107 所示。

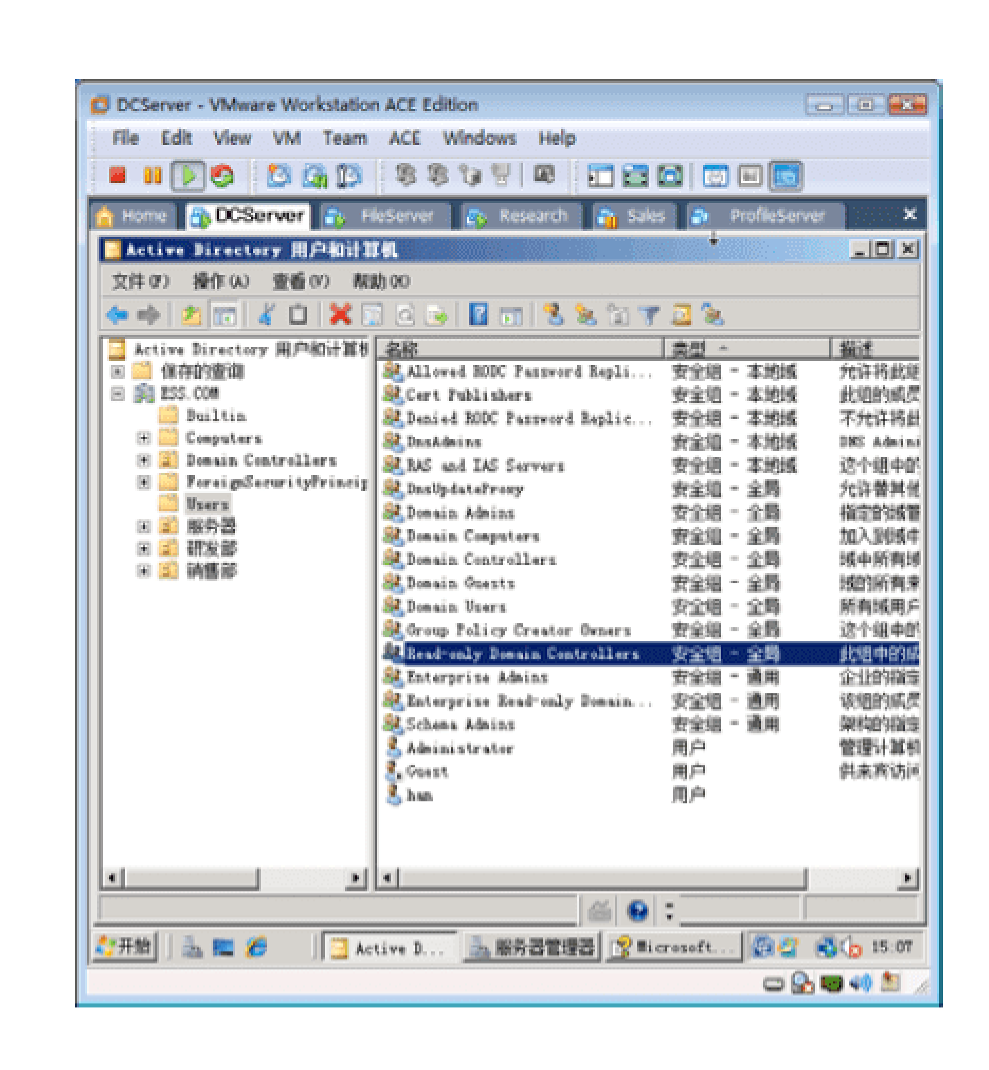


图 5-107 内置的全局组

- Domain Admins：该域内的成员计算机会自动将该组加入到其 Administrators 组中，因此 Domain Admins 这个全局组内的每个成员都具备系统管理员的权限。该组默认的成员为域用户 Administrators。
- Domain Computers：所有加入该域的计算机都被自动加入到该组内。
- Domain Controllers：域内所有域控制器都被自动加入到该组内。
- Domain Users：域内的成员计算机会自动将该组加入到其 Users 组内。该组默认的成员为域用户 Administrator，而后，所有添加的域用户账户都自动属于该 Domain Users 全局组。

- Domain Guests：Windows Server 2008 会自动将该组加入到 Guest 本地域组内。该组默认的成员为用户账户 Guest。
- Enterprise Admins：该组只存在于域整理目录林的根域中，其成员具有管理整个目录林内的所有域的权利。
- Schema Admins：该组只存在于域整理目录林的根域中，其成员具备管理架构的权利。
- Group Policy Creator Owners：该组中的成员可以修改域的组策略。
- Read-only Domain Controllers：此组中的成员是域中只读域控制器。

5.6.6　示例：在域中使用组简化授权

在单域环境中使用 A→G→DL→P 授权策略。

以下操作将创建两个全局组“研发人员”和“销售人员”即分别合并研发部门和销售部门的用户账户，再创建一个“公共空间访问组”本地域组，并授予其访问 Research 计算机上的“公共空间”文件夹的访问和修改权限。以后如果研发人员或销售人员需要访问“公共空间”文件夹，只需将其加入到“公共空间访问组”即可。这样授权某类人群访问资源就变成了将用户添加到本地域组的过程。

① 登录 DCServer，打开“Active Directory 用户和计算机”窗口。

② 如图 5-108 所示，右击“研发部”的“用户”组织单元，在弹出的快捷菜单中选择“新建”→“组”命令。

③ 如图 5-109 所示，在出现的“新建对象-组”对话框中，输入组的名称“研发人员”，组的类型选择“安全组”，单击“确定”按钮。

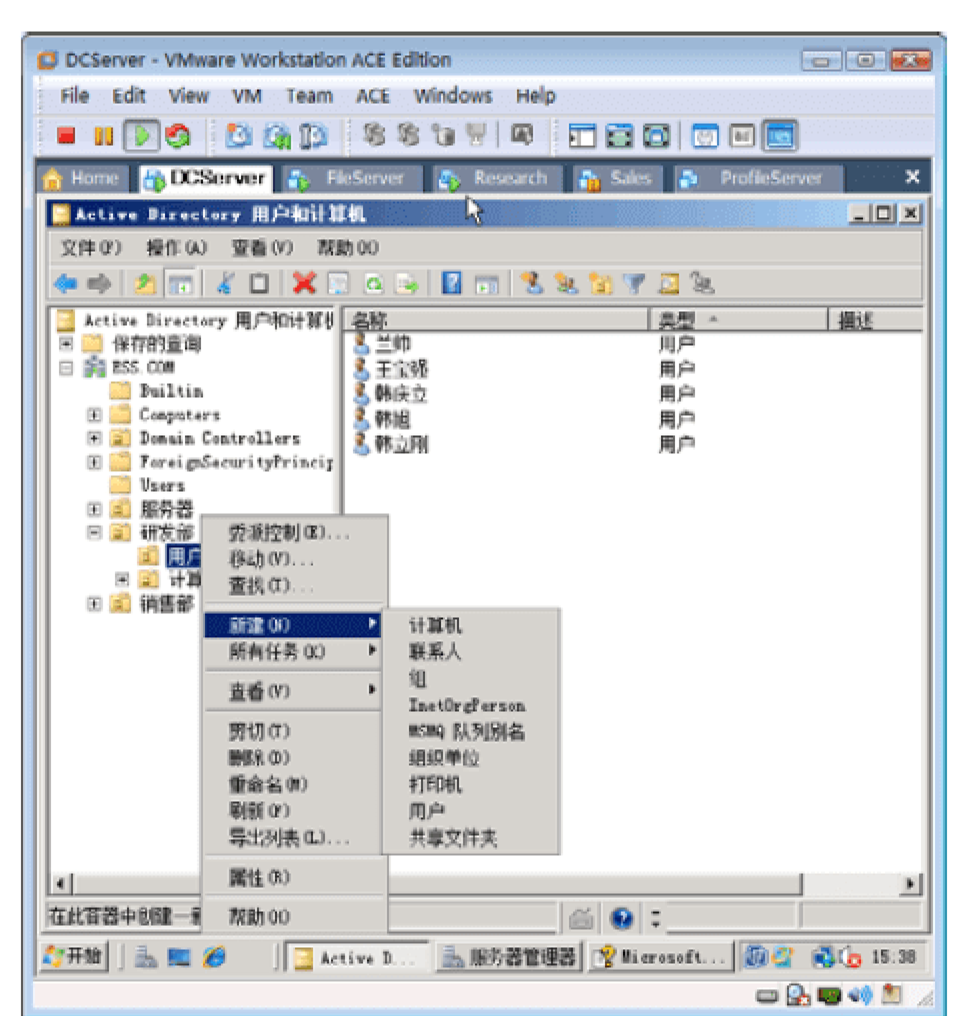
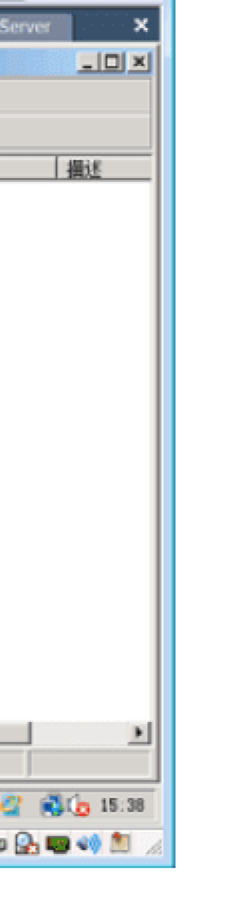



图 5-108　创建全局组

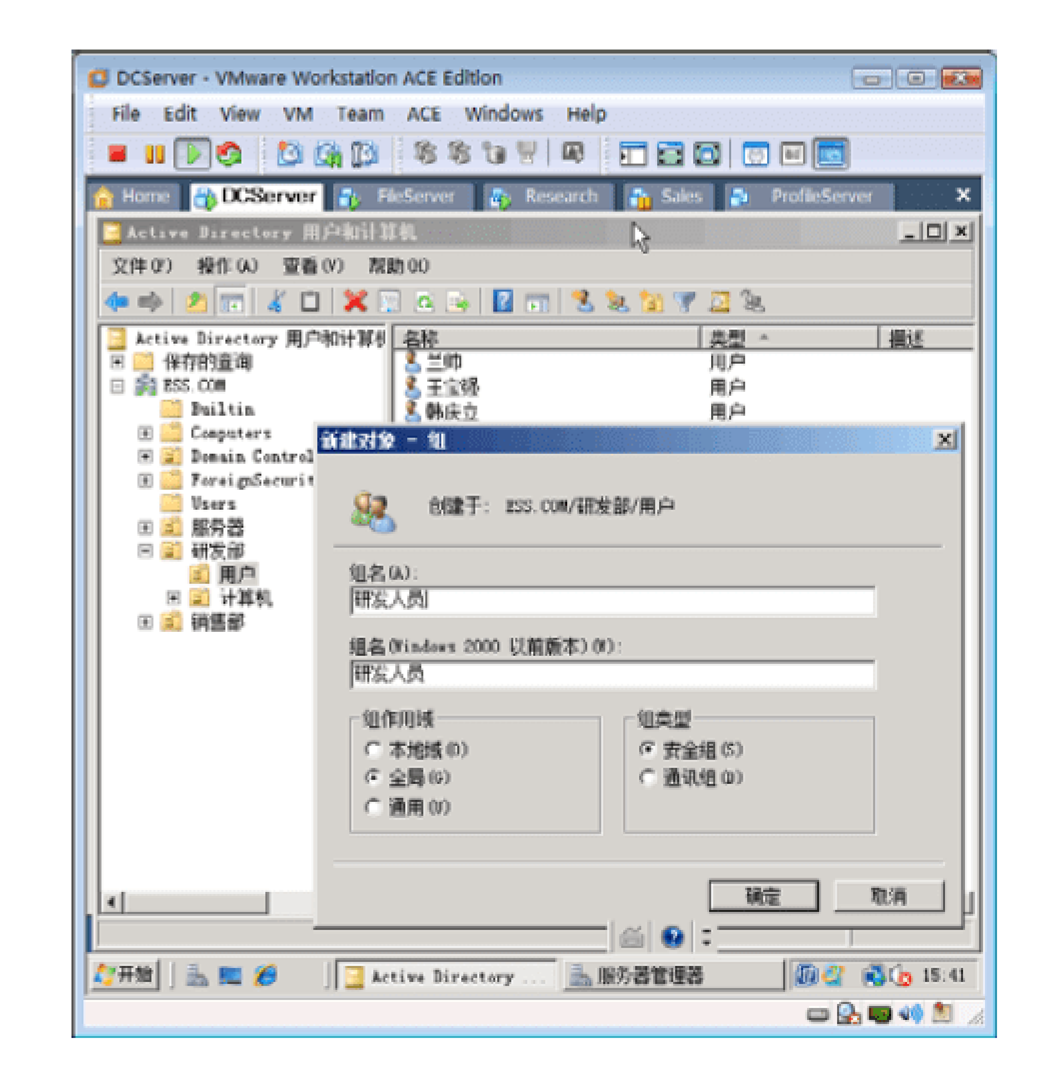


图 5-109　指定组的类型和作用域以及名称

④ 如图 5-110 所示，选中研发部门的用户账户，右击选中的用户，在弹出的快捷菜单中选择“添加到组”命令。

⑤ 如图 5-111 所示，在出现的对话框中，输入“研发人员”，单击“确定”按钮。

⑥ 按照以上步骤，创建“销售人员”全局组。将销售部的用户账户添加到“销售人员”组。

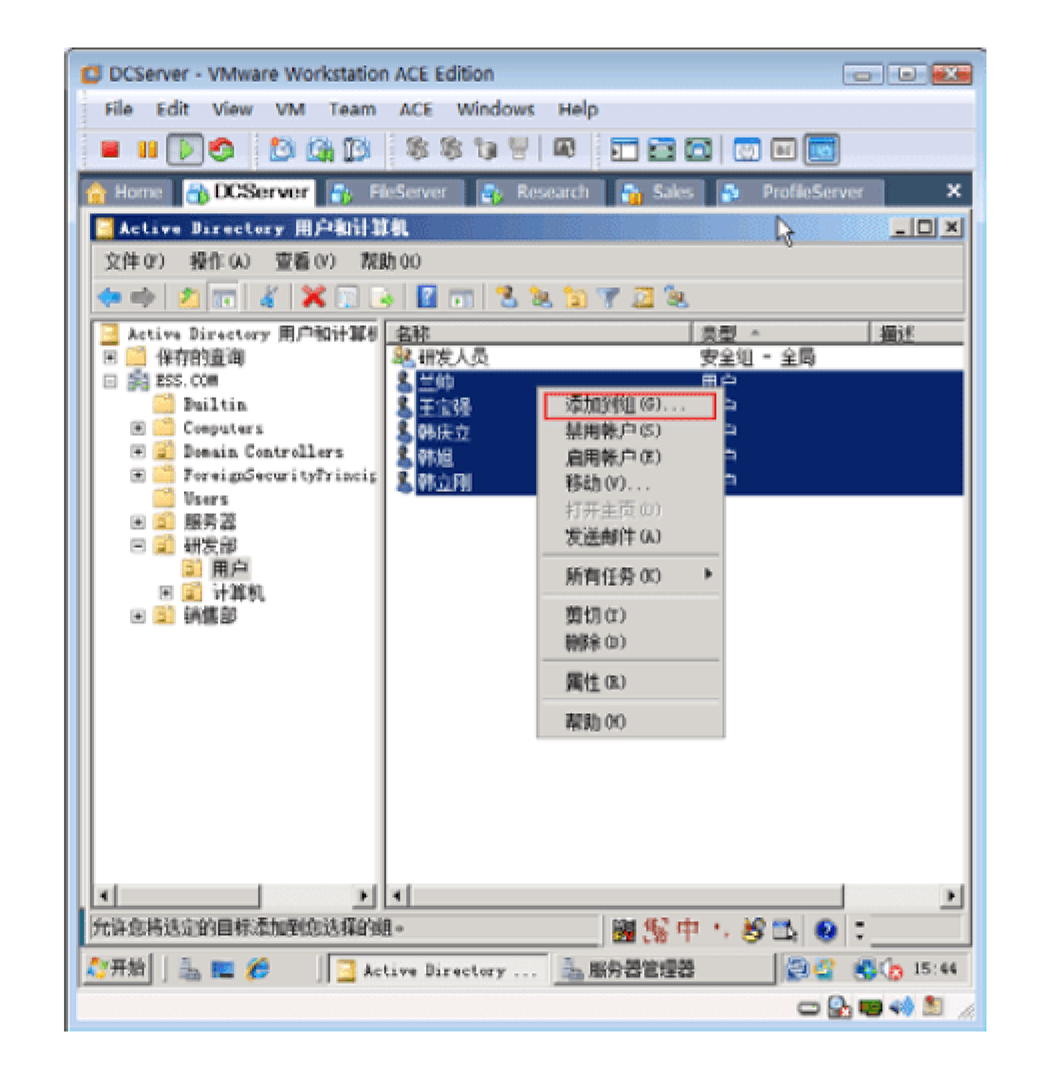


图 5-110 选定用户

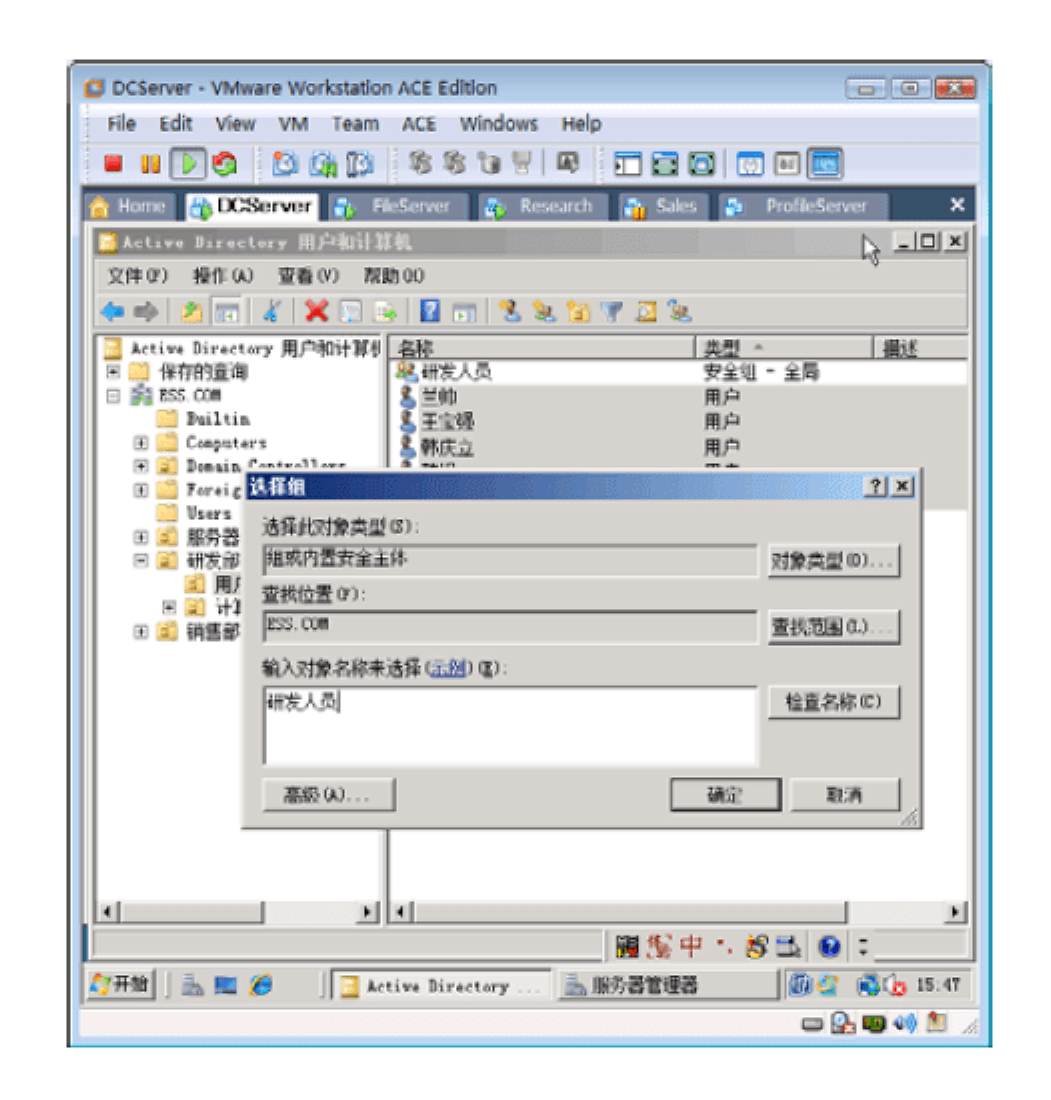


图 5-111 将用户添加到全局组

⑦ 如图 5-112 所示，创建一个本地域组“公共空间访问组”。

⑧ 如图 5-113 所示，以域管理员身份登录 Research 计算机，右击 C 盘下的“公共空间”，在弹出的快捷菜单中选择“属性”命令。切换到“安全”选项卡，单击“编辑”按钮。

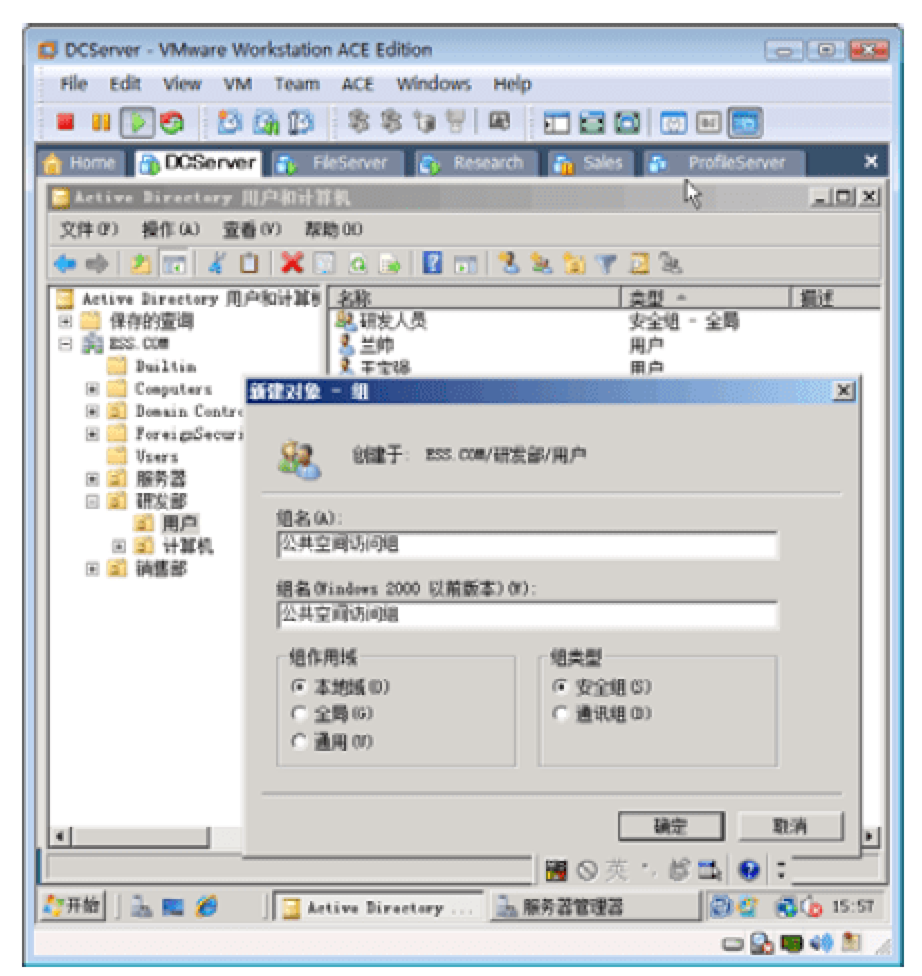


图 5-112 创建本地域组

图 5-113 授权对共享文件夹的访问

⑨ 如图 5-114 所示，在出现的对话框中，输入“公共空间访问组”，单击“检查名称”按钮。单击“确定”按钮。

⑩ 如图 5-115 所示，授予其修改、读取和执行、列出文件夹目录和读取的权限。

⑪ 如图 5-116 所示，在 DCServer 上，将“销售人员”全局组添加到“公共空间访问组”，就等于授予销售人员访问公共空间的权限。

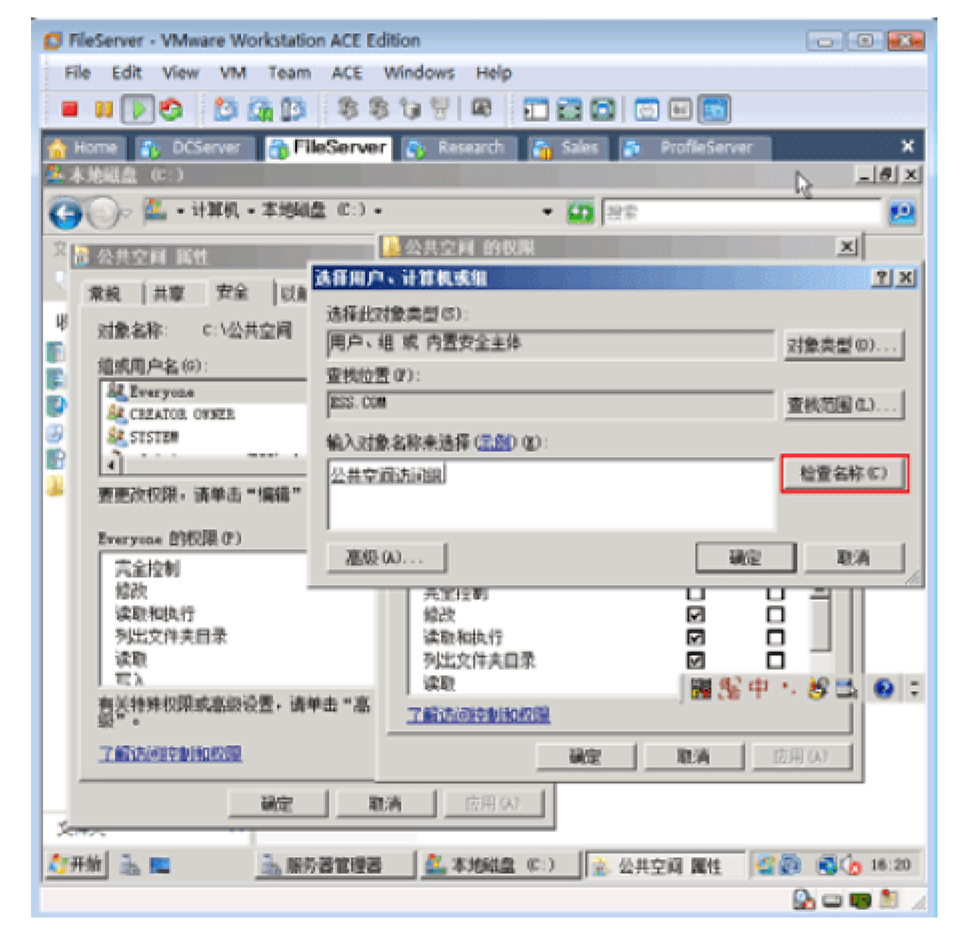




图 5-114　为本地域组授权

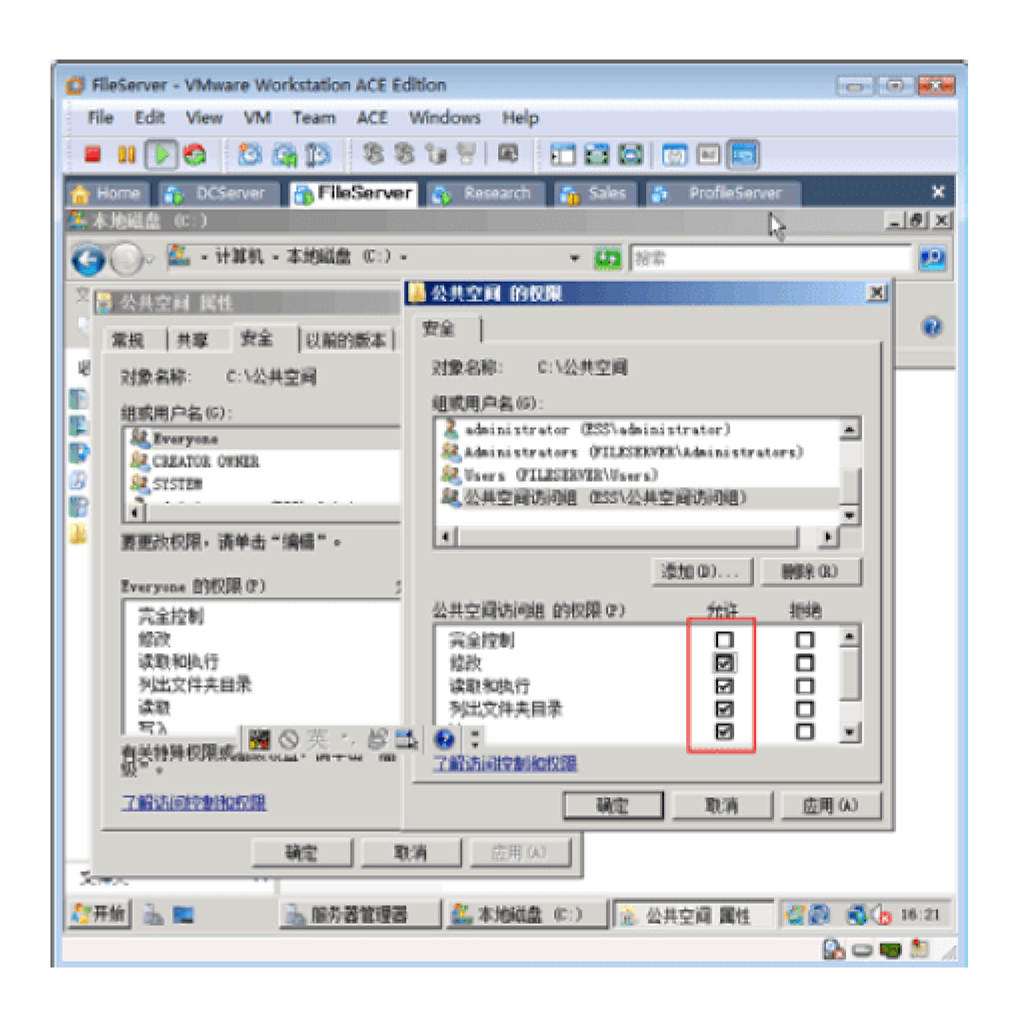


图 5-115　指定访问权限

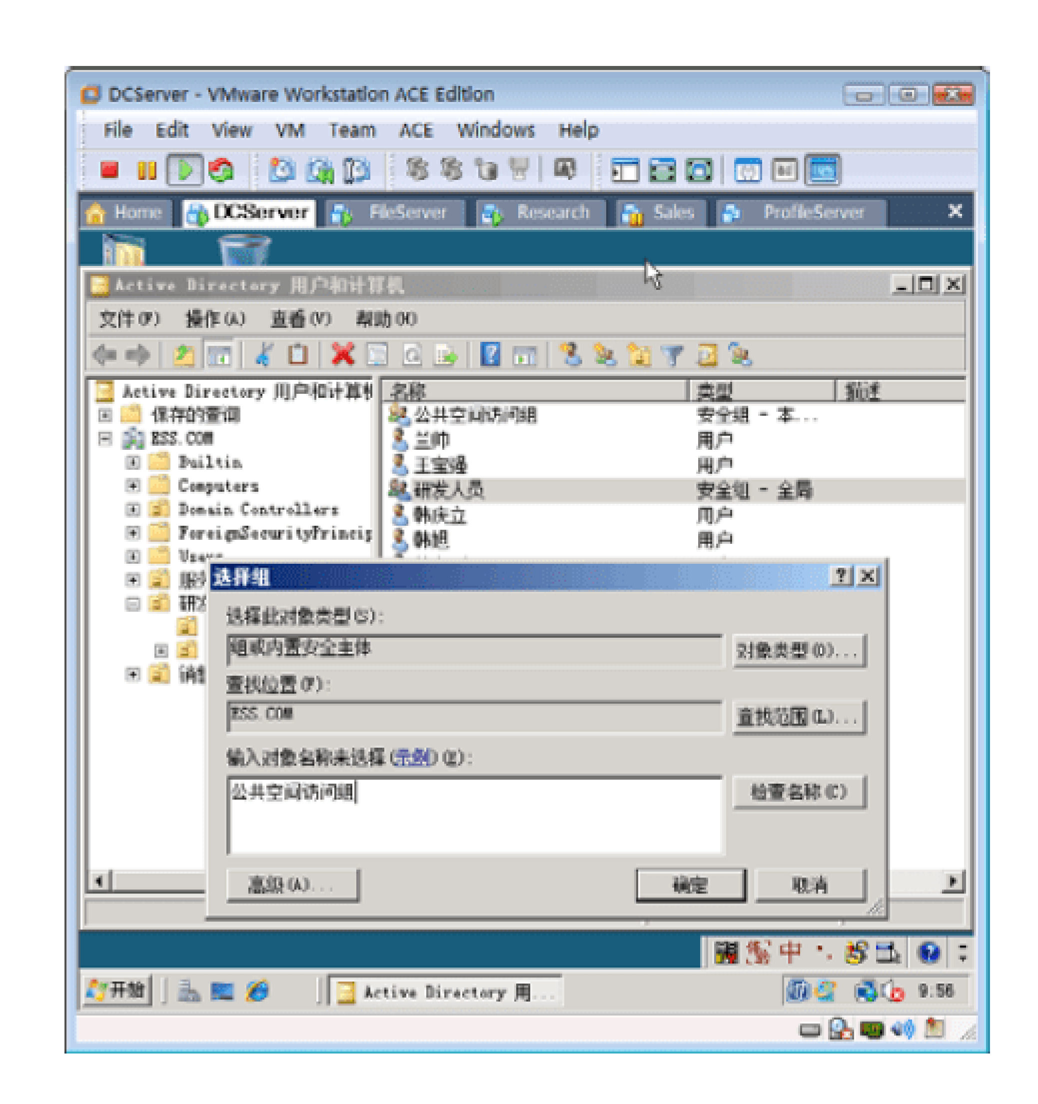


图 5-116　将全局组添加到本地域组



提示：现在授权用户访问“公共空间”文件夹的过程，就变成了将用户或组加入“公共空间访问组”的过程，省去了步骤 7~9 的操作，使得授权过程简化，这就是使用 A→G→DL→P 策略的好处。

第 6 章　利用 NTFS 管理数据

NTFS 是 Windows NT 操作系统使用的文件系统，Windows 2000、Windows 2003、Windows 2008、Windows XP 及 Vista 都能创建 NTFS 分区。

NTFS 分区与 FAT32 分区相比有较大的优势，本章将基于此展开内容。

关键词

- NTFS 分区和 FAT32 分区的区别
- 将 FAT32 分区转化成 NTFS 分区
- 利用 NTFS 权限
- 利用特殊的 NTFS 权限
- 利用 EFS 保护数据安全
- 在 NTFS 分区上压缩数据
- 配置 NTFS 分区上的磁盘限额
- 配置卷影副本

6.1 FAT32 和 NTFS

6.1.1 FAT32

FAT32 实际上是文件分区表采用的一种格式，它是相对于 FAT16 而言的。众所周知，DOS 和 Windows 95 采用的都是 FAT16 格式。那么为什么一定要推出 FAT32 呢？这主要是由其自身的优越性所决定的。

首先，它可以大大地节约磁盘空间。文件在磁盘上是以簇的方式存放的，簇里存放了一个文件后就不能再存放另外的文件。假如一个磁盘的分区大小为 512MB，基于 FAT16 系统的簇的大小为 8KB，而 FAT32 系统的簇的大小仅为 4KB，那么，存放一个 3KB 的文件，FAT16 系统就会有 5KB 的空间被浪费，而 FAT32 浪费的则会少一些。如果分区达到 1GB，FAT16 的簇的大小为 16KB，而 FAT32 还是 4KB，节省的空间也就更多了。

其次，在推出 FAT32 文件系统之前，通常 PC 使用的文件系统是 FAT16。像基于 MS-DOS、Windows 95 等系统都采用了 FAT16 文件系统。在 Windows 9x 下，FAT16 支持的分区最大为 2GB。我们知道计算机将信息保存在硬盘上称为“簇”的区域内。使用的簇越小，存储效率就越高。在 FAT16 的情况下，分区越大簇就相应的要增大，存储效率就越低，势必造成存储空间的浪费。并且随着计算机硬件和应用水平的不断提高，FAT16 文件系统已不能很好地适应系统的要求。在这种情况下，推出了增强的文件系统 FAT32。与 FAT16 相比，FAT32 主要具有以下优点。

- 可以支持的磁盘大小达到 2TB(2048GB)，但是不能支持小于 512MB 的分区。基于 FAT32 的 Win 2000 可以支持的分区最大为 32GB；而基于 FAT16 的 Windows 2000 支持的分区最大为 4GB。
- 由于采用了更小的簇，FAT32 文件系统可以更有效率地保存信息。如两个分区大小都为 2GB，一个分区采用 FAT16 文件系统，另一个分区采用 FAT32 文件系统，采用 FAT16 的分区的簇大小为 32KB，而 FAT32 分区的簇只有 4KB，这样 FAT32 就比 FAT16 的存储效率要高很多。通常情况下可以提高 15%。
- FAT32 文件系统可以重新定位根目录和使用 FAT 的备份副本。另外，FAT32 分区的启动记录被包含在一个含有关键数据的结构中，减少了计算机系统崩溃的可能性。

6.1.2 NTFS

NTFS 是 Windows NT 操作环境和 Windows NT 高级服务器网络操作系统环境的文件系统。NTFS 的目标是：提供可靠性，通过可恢复能力(事件跟踪)和热定位的容错特征来实现；增加功能性的一个平台；对 POSIX 需求的支持；消除 FAT 和 HPFS(High Performance File System 是微软为 OS/2 1.2 设计的)，支持局域网管理的文件服务器。

NTFS 提供长文件名、数据保护和恢复，并通过目录和文件许可实现安全性。NTFS 支持大硬盘和在多个硬盘上存储文件(称为跨越分区)。例如，一个大公司的数据库可能大得必须跨越不同的硬盘。NTFS 提供内置安全性特征，它控制文件的隶属关系和访问。从 DOS 或其他操作系统上不能直接访问 NTFS 分区上的文件。如果要在 DOS 下读/写 NTFS 分区文件的话，则可以借助第三方软件；至今(2007 年 5 月)在 Linux 下一般只能读取而不能写入 NTFS 分区文件。这是 Windows NT 安全性系统的一部分，但是，只有在使用 NTFS 时才是这样的。

NTFS 允许文件名的长度可达 256 个字符。虽然 DOS 用户不能访问 NTFS 分区，但是 NTFS 文件可以复制到 DOS 分区。每个 NTFS 文件都包含一个可被 DOS 文件名格式认可的 DOS 可读文件名。该文件名是 NTFS 从长文件名的开始字符中产生的。

与 FAT32 分区相比 NTFS 分区有以下优点。

- NTFS 权限。
- 加密文件系统(EFS)。
- 磁盘压缩。
- 磁盘限额。
- 卷影副本。

6.2　将 FAT32 分区转化成 NTFS 分区

将 FAT32 文件分区转化成 NTFS 分区数据不会丢失。如果转化的分区是系统分区或虚拟内存使用的磁盘分区，需要重启才能转化。下面在 FileServer 上的操作将会创建一个 FAT32 的磁盘分区，然后将其转化成 NTFS 分区。

① 在文件服务器 FileServer 计算机上，以管理员的身份登录，打开“服务器管理器”窗口。

② 展开“存储”→“磁盘管理”节点。如图 6-1 所示，右击未分配的磁盘空间，在弹出的快捷菜单中选择“新建简单卷”命令。

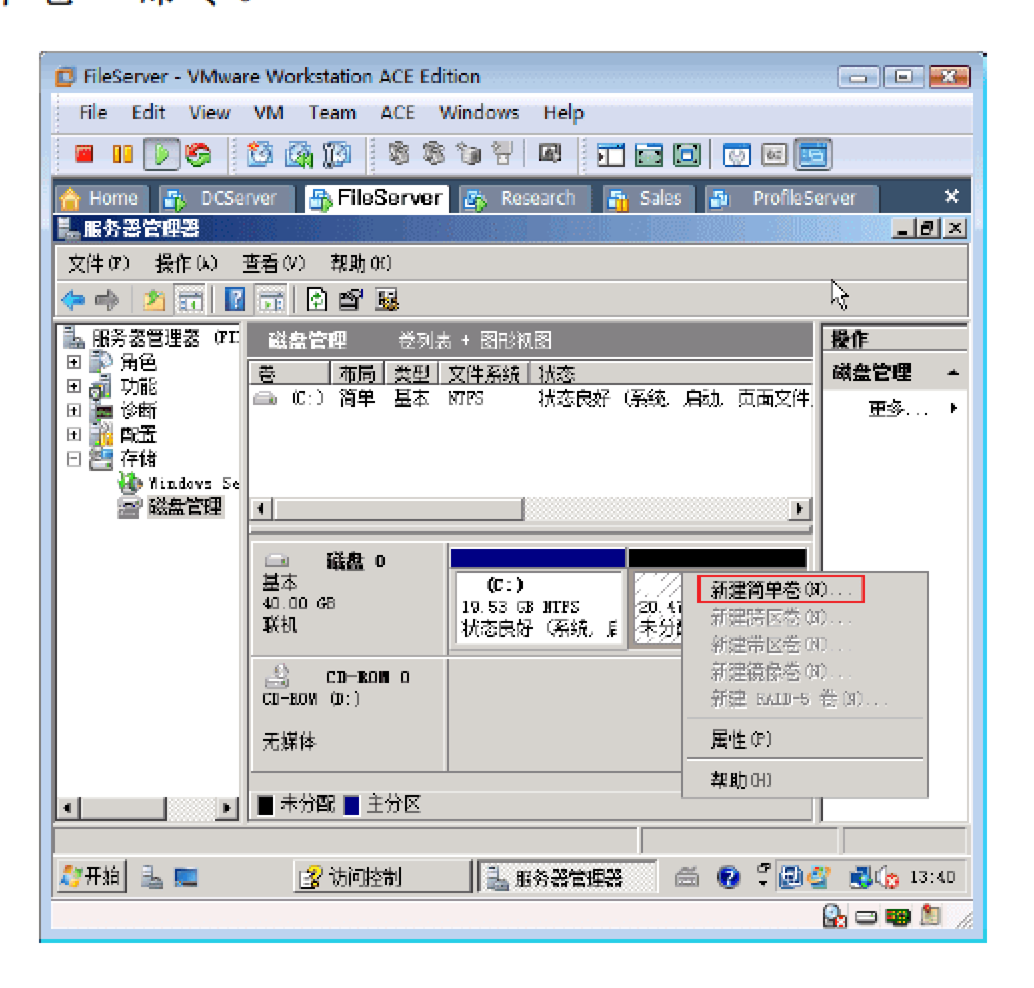


图 6-1　创建简单卷

③ 在出现的向导中，单击“下一步”按钮。

④ 在出现的“指定卷大小”界面中，如图 6-2 所示，输入卷的大小，默认是剩余大小，单击“下一步”按钮。

⑤ 如图 6-3 所示，在出现的“分配驱动器号和路径”界面中，指定驱动器号，单击“下一步”按钮。

⑥ 选中“按下列设置格式化这个卷”单选按钮，文件系统选择 FAT32，选中“执行快速格式化”复选框，如图 6-4 所示。

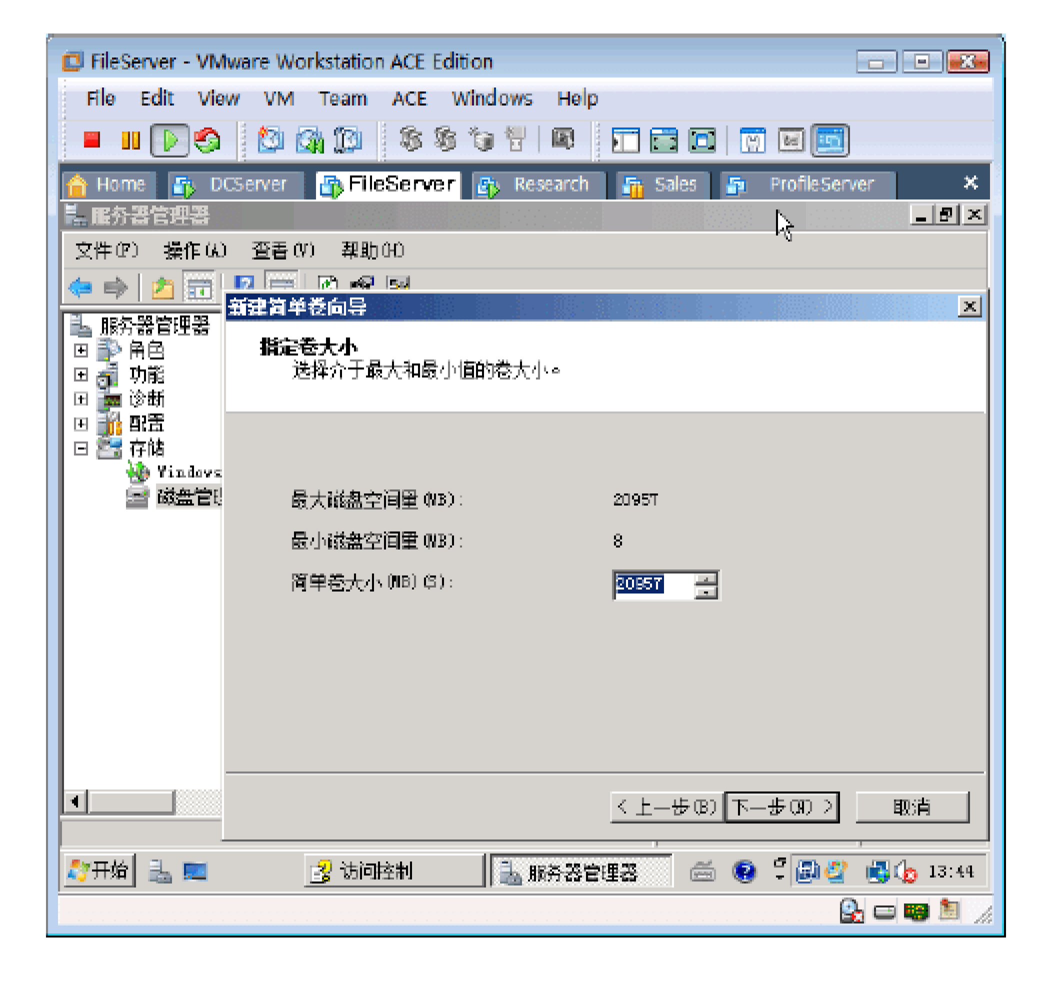


图 6-2　指定卷的大小

图 6-3　指定盘符

⑦　完成新建简单卷向导。

⑧　如图 6-5 所示，可以通过磁盘管理和磁盘属性查看磁盘的文件系统。

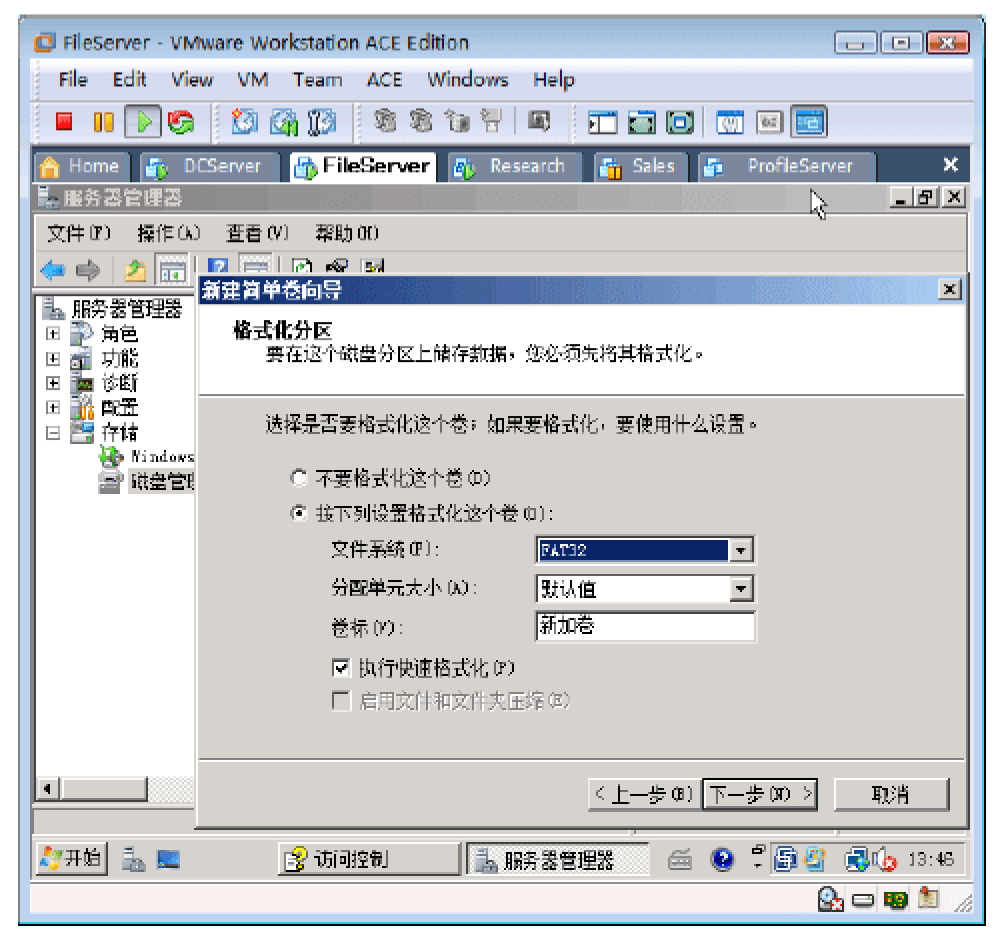


图 6-4　选择文件系统

图 6-5　查看文件系统

⑨　如图 6-6 所示，也可以通过卷的属性查看卷的文件系统。

⑩　如图 6-7 所示，在命令行输入以下命令将其转化成 NTFS 分区。输入 convert e:/fs:ntfs 和卷标“新加卷”，按 Enter 键。

注意：转换系统卷，需要重启，在启动时转化。如果要转化的卷有虚拟内存，也需要重启。这种转化数据不会丢失。不能从 NTFS 转化成 FAT32，可以使用 FAT32 文件系统格式化 NTFS 分区，这种转化数据会丢失。

⑪　如图 6-8 所示，转化完成后从磁盘管理器看到 E 卷已经转化成了 NTFS 分区。

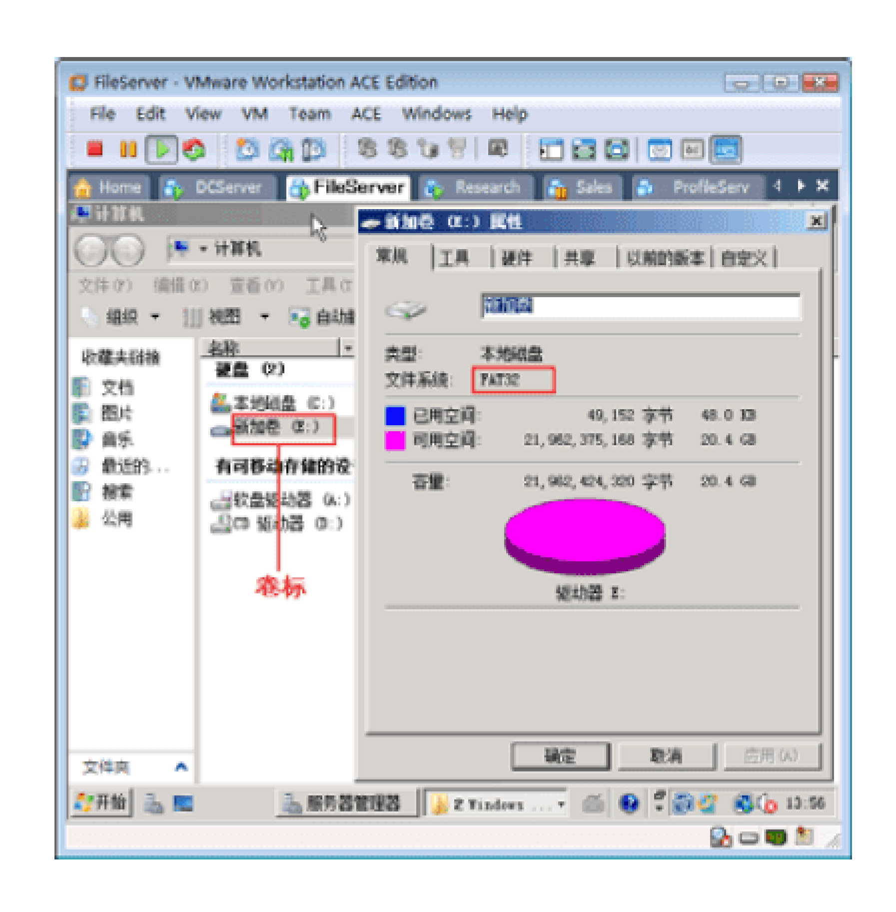


图 6-6　查看卷的文件系统

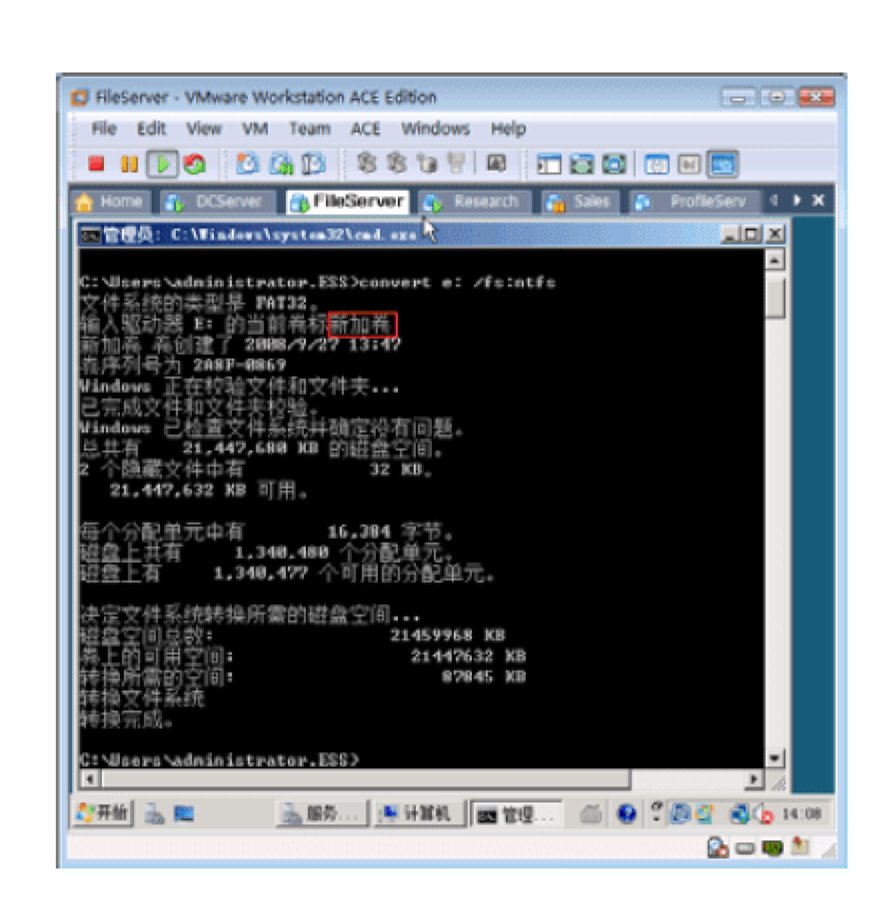


图 6-7　转化成 NTFS

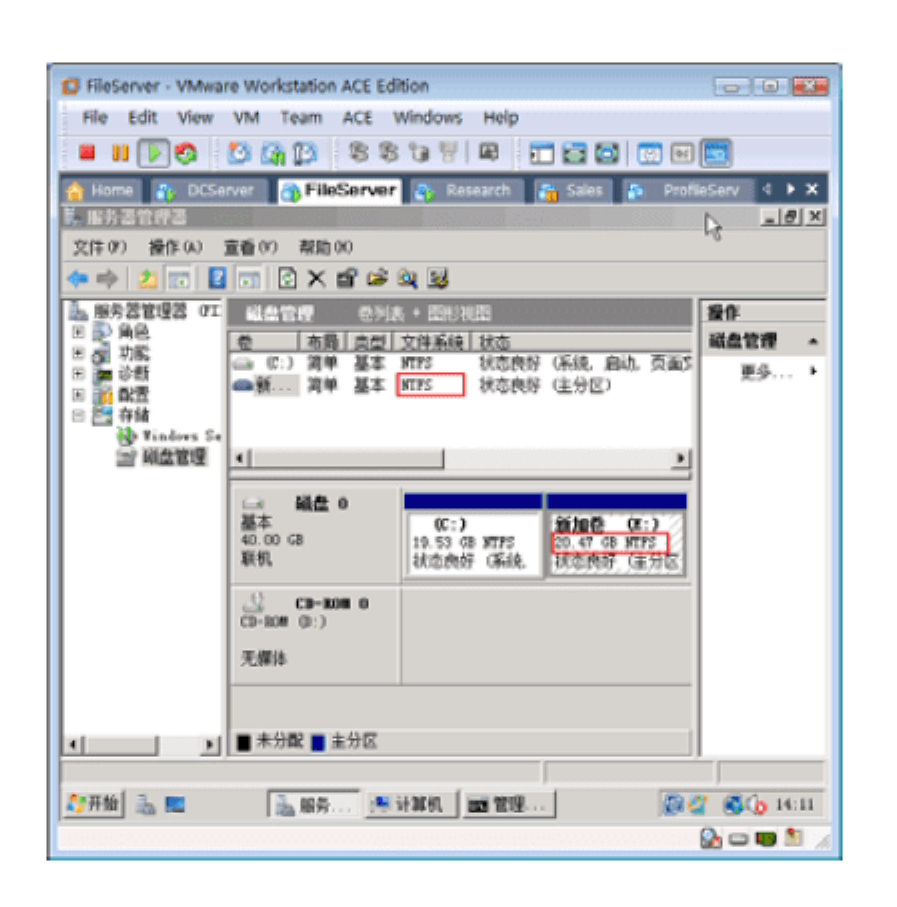


图 6-8　查看文件系统

6.3　NTFS 权限

存储在 NTFS 分区上的文件和文件夹对用户的访问有安全控制，可以控制用户访问的级别。比如，只允许读取不能更改，或者只允许列出文件夹内容，不允许打开其中的文件等。

6.3.1　NTFS 权限介绍

当一个用户试图访问一个文件或者文件夹的时候，NTFS 文件系统会检查用户使用的账户或者账户所属的组是否在此文件或文件夹的访问控制列表(ACL)中。如果存在，则进一步检查访问控制项(ACE)，然后根据控制项中的权限来判断用户最终的权限。如果访问控制列表中不存在用户使用的账户或者账户所属的组，则拒绝用户访问。

1. 文件夹的 NTFS 安全权限

- 完全控制：对文件或者文件夹可执行所有操作。

- 修改：可以修改、删除文件或者文件夹。
- 读取和运行：可以读取内容，并且可以执行应用程序。
- 列出文件夹目录：可以列出文件夹内容，此权限只针对文件夹存在。
- 读取：可以读取文件或者文件夹的内容。
- 写入：可以创建文件或者文件夹。
- 特别的权限：其他不常用权限，比如删除权限的权限。

2. 文件的 NTFS 安全权限

所有权限都有相应的“允许”和“拒绝”两种选择。文件或者文件夹的默认权限是继承上一级文件夹的权限，如果是根目录(比如 c:\)下的文件夹，则其权限是继承磁盘分区的权限，如图 6-9、图 6-10 所示。

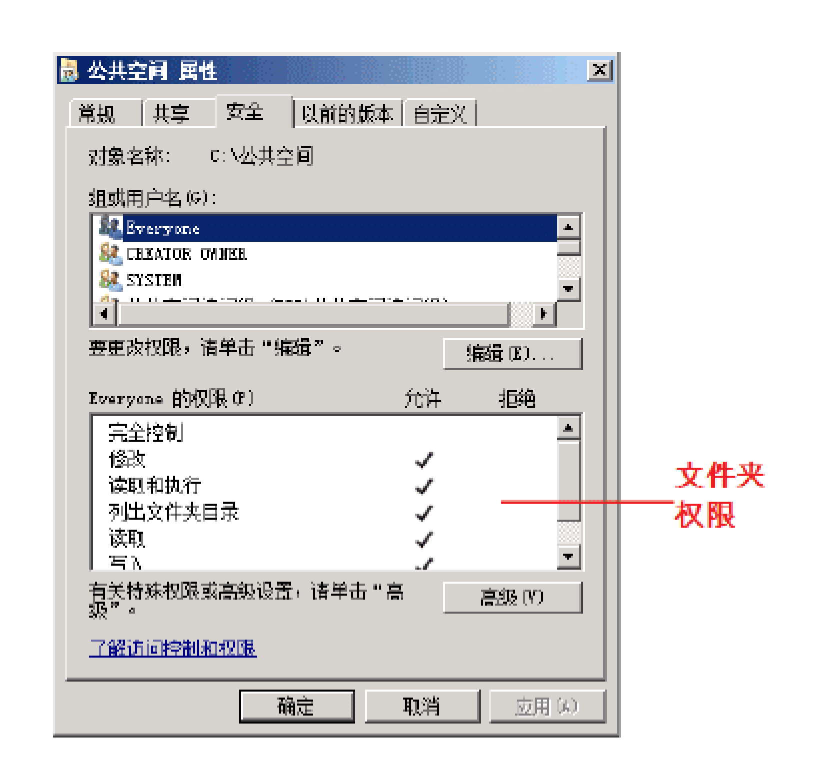


图 6-9　文件夹权限

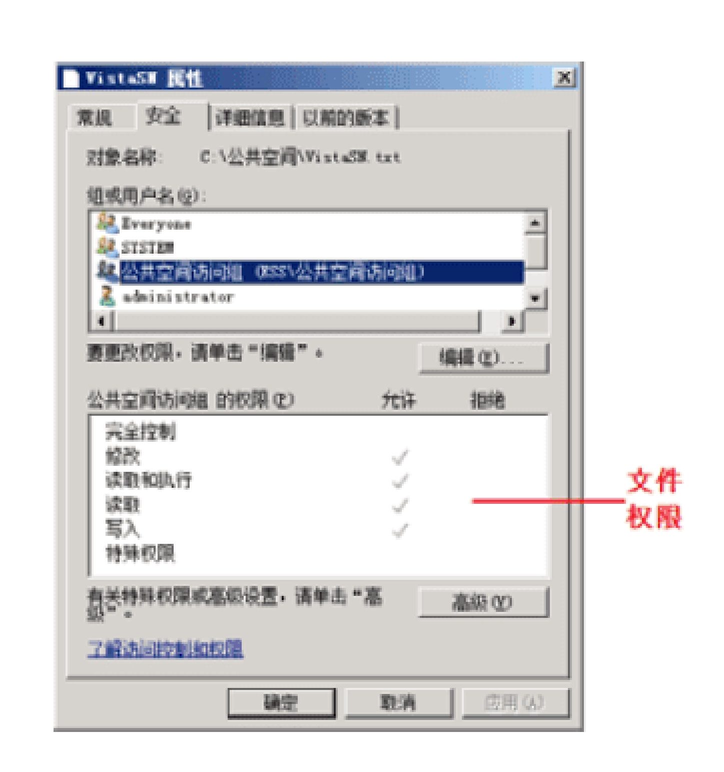


图 6-10　文件权限

6.3.2　NTFS 权限的应用规则

下面介绍 NTFS 安全权限的应用规则。

1. 权限是累加的

当一个用户属于多个组的时候，这个用户会得到各个组的累加权限，但是一旦有一个组的相应权限被拒绝，此用户的此权限也会被拒绝。比如：假设有一个用户 USER，如果 USER 属于 A 和 B 两个组，A 组对某文件有读取权限，B 组对此文件有写入权限，USER 自己对此文件有修改权限，那么 USER 对此文件的最终权限为读取+写入+修改权限。

2. 权限的继承

新建的文件或者文件夹会自动继承上一级目录或者驱动器的 NTFS 权限，但是从上一级继承下来的权限是不能直接修改的，只能在此基础上添加其他权限。也就是不能把权限上的勾去掉。

当然这并不是绝对的，只要有足够的权限，比如你是管理员，也可以修改这个继承下来的权限，或者让文件不再继承上一级目录或者驱动器的 NTFS 权限。

3. 权限的拒绝

拒绝的权限优先于允许的权限。无论给用户账户什么权限，只要设置了拒绝权限，那么被拒绝的权限就绝对有效。

4．移动和复制操作对权限的影响

这里一共有 3 种情况，同一 NTFS 分区、不同 NTFS 分区以及 FAT 分区，如表 6-1 所示。

表 6-1　移动和复制操作对权限的影响

	同一 NTFS 分区	不同 NTFS 分区	FAT 分区
移动	继承目标文件(夹)权限	继承目标文件(夹)权限	丢失权限
复制	保留源文件(夹)权限	继承目标文件(夹)权限	丢失权限

6.3.3　显式权限和继承权限

一般对象有两种类型的权限：显式权限和继承权限。

- 显式权限是创建对象时用户所设置的默认权限。
- 继承权限是从父对象传播到子对象的权限。继承权限使管理权限的任务更加容易，并且确保给定容器内所有对象权限的一致性。

默认情况下，容器内的对象从创建该对象时的容器继承权限。例如，创建名为“公共空间”的文件夹时，“公共空间”内的所有子文件夹和文件都自动从该文件夹继承权限。因此，“公共空间”文件夹有显式权限，而其内部的所有子文件夹和文件都有继承权限。

示例：查看继承的权限。

如图 6-11 所示，打开在 FileServer 服务器的“公共空间”文件夹下的记事本文件 VistaSN.txt 属性，切换到“安全”选项卡，单击“高级”按钮。

如图 6-12 所示，在出现的“VistaSN 的高级安全设置”对话框中，能够看到从父项继承下来的权限。

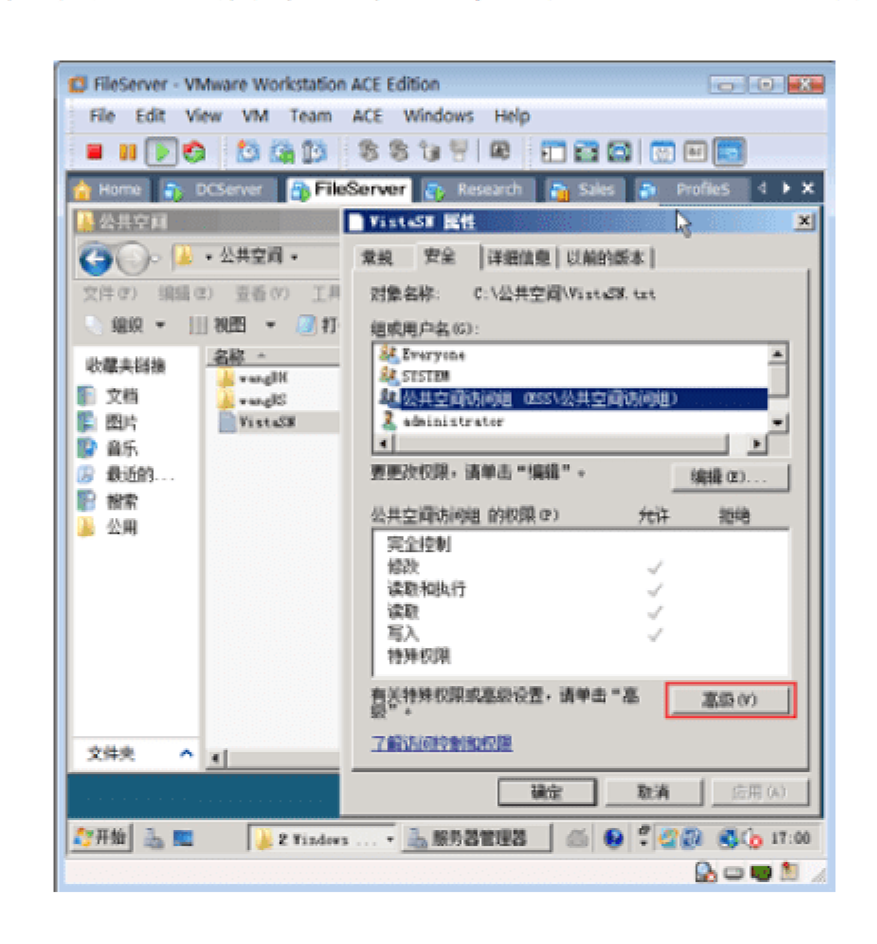



图 6-11　查看高级权限

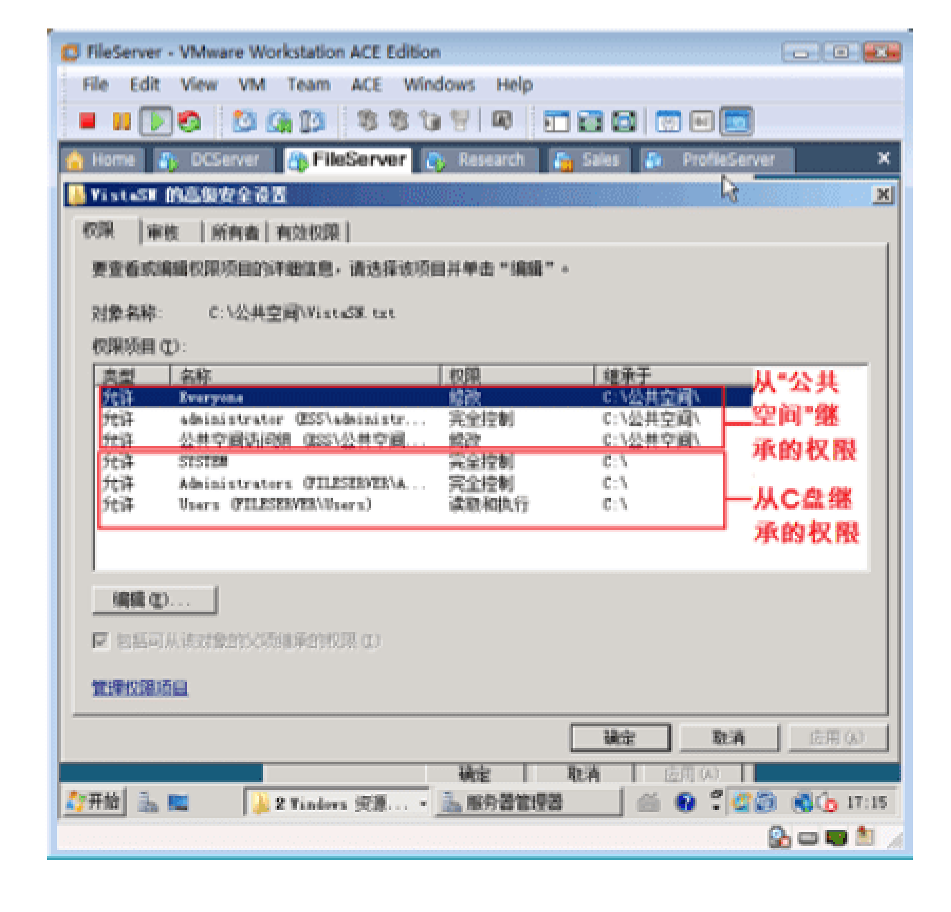


图 6-12　查看继承下来的权限


注意：如果对象有显式“允许”权限项，则继承的“拒绝”权限并不会阻止对该对象的访问。显式权限的优先级高于继承权限，即使继承的是“拒绝”权限。继承的权限默认不能更改，除非阻止该文件或文件夹继承父项的权限。

6.3.4 确定应用权限的位置

当在父文件夹上设置权限后，在该文件夹中创建的新文件和子文件夹都将继承这些权限。如果不想让它们继承这些权限，则在设置父文件夹的特殊权限时应选择“应用于”框中的“仅此文件夹”选项。

示例： 更改权限的应用位置。

将“公共空间访问组”的访问权限应用到文件夹以及子文件夹，不应用到内部的文件。

① 如图 6-13 所示，打开“公共空间”文件夹属性，切换到“安全”选项卡，单击“高级”按钮。

② 如图 6-14 所示，在高级安全对话框中，查看“公共空间访问组”的权限应用于：该文件夹，子文件和文件，单击“编辑”按钮。

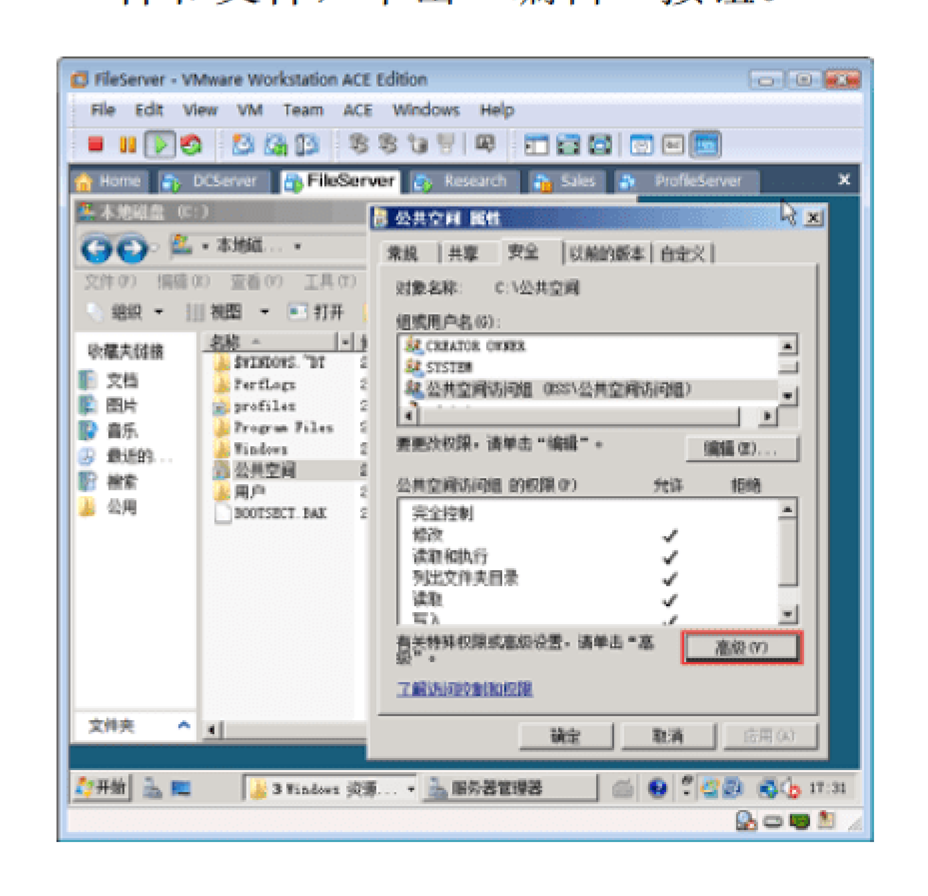


图 6-13 查看高级权限设置

图 6-14 查看权限应用层次

③ 如图 6-15 所示，可以看到在文件夹上设置的权限默认应用到该文件夹、子文件夹和文件。

④ 在高级安全设置对话框中，选中“公共空间访问组”选项，单击“编辑”按钮。

⑤ 如图 6-16 所示，在出现的权限项目对话框中，在“应用于”下拉列表框中选择“该文件夹及子文件夹”选项，单击“确定”按钮，完成更改。

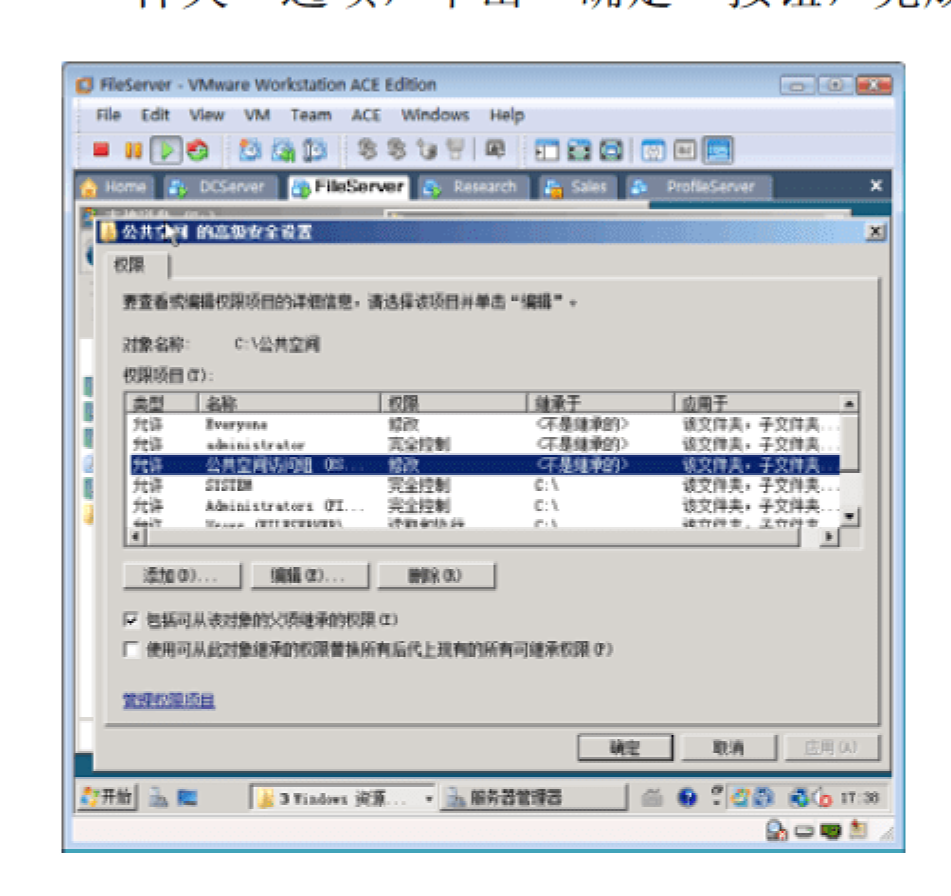


图 6-15 编辑高级权限

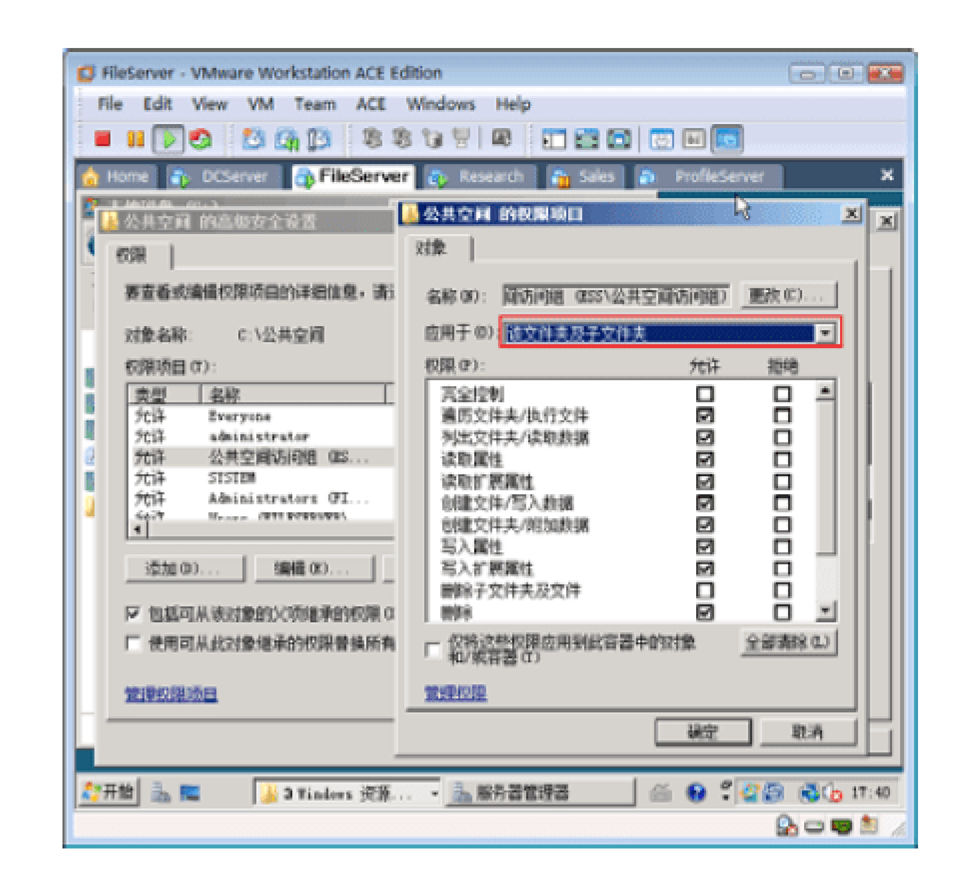


图 6-16 更改权限应用层次

⑥　如图 6-17 所示，再次打开“公共空间”内的记事本文件，查看其安全属性。

⑦　如图 6-18 所示，打开其中的文件夹查看权限的应用情况。



提示：你将发现记事本文件没有应用“公共空间访问组”的权限，而文件夹应用了“公共空间访问组”的权限。

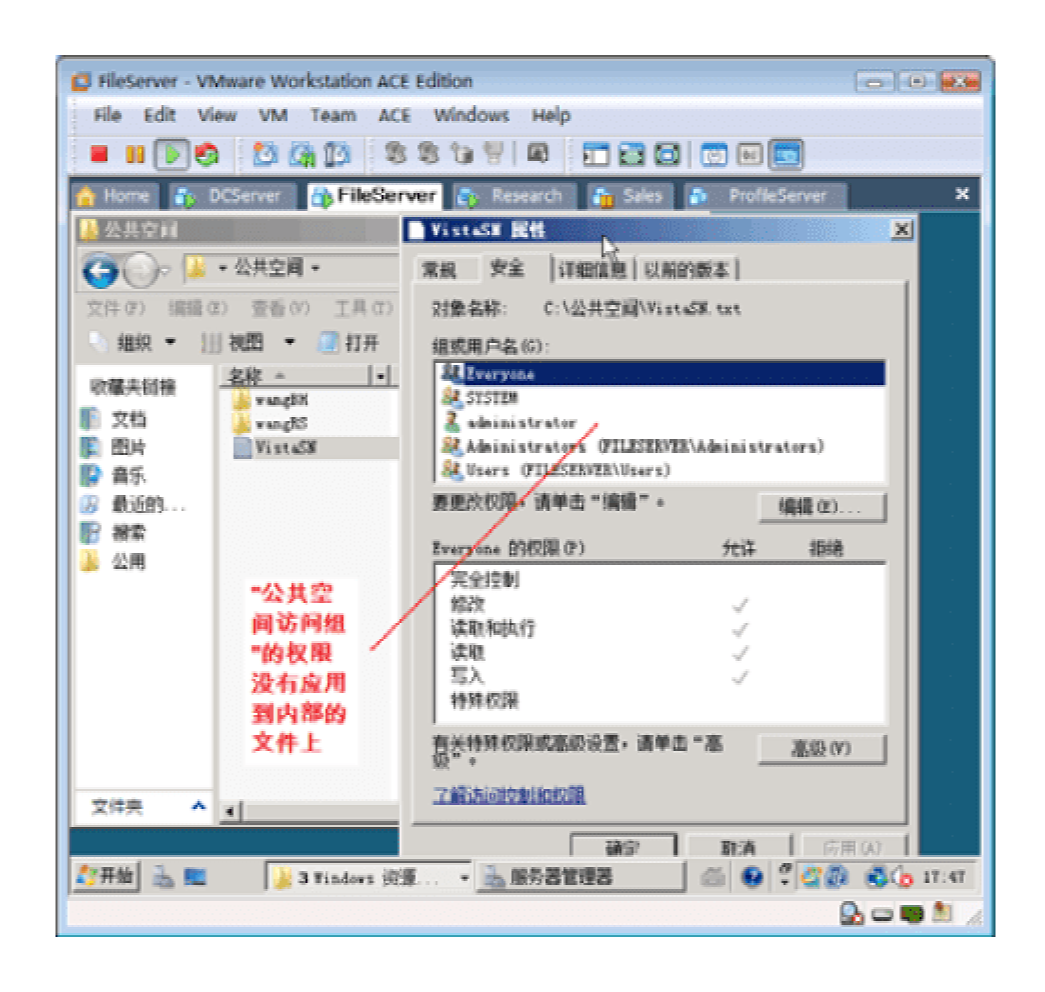


图 6-17　检查文件的权限继承情况

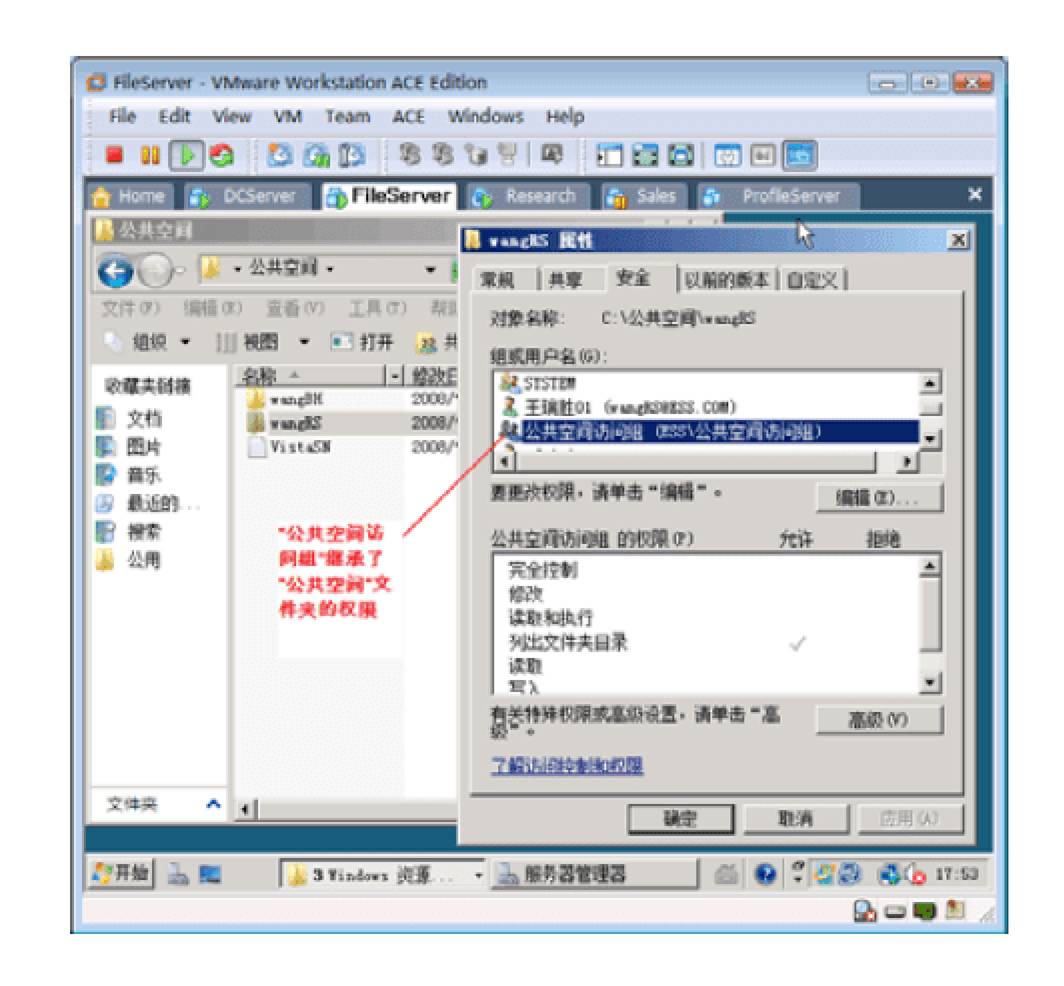


图 6-18　检查文件夹的权限继承情况

6.3.5　阻止应用继承权限

可以通过“权限”选项卡更改特殊权限。如果要阻止某些文件或子文件夹继承权限，则右击该文件或子文件夹，在弹出的快捷菜单中选择“属性”命令，切换到“安全”选项卡，单击“高级”按钮，然后取消选中“包括可从此对象的父项继承的权限”复选框。

如果与每个权限相关联的“允许”或“拒绝”复选框显示为被阴影覆盖，则表示文件或文件夹已经从父文件夹中继承了权限。有三种方法可以更改继承的权限。

(1) 选择相反的权限(“允许”或“拒绝”)替代继承的权限，如图 6-19 所示。

示例 1：选择相反的权限替代继承权限。

在 VistaSN.txt 记事本文件的安全属性上可以看到继承下来的权限，Administrators 组有完全控制的权限，继承下来的权限在这个地方不能修改，但是可以选择拒绝“读取和执行”和“读取”的权限，这样就会用相反的权限替代继承的权限。

(2) 取消选中“包括可从该对象的父项继承的权限”复选框。

这样，你就可以更改权限，或者从权限列表中删除用户或组。但是，文件或文件夹将不再从父文件夹继承权限。

示例 2：去掉继承的权限。

如果想完全重新设置 VistaSN.txt 记事本的权限，则可以去掉继承下来的权限。

①　打开记事本“VistaSN 属性”对话框，如图 6-20 所示，切换到“安全”选项卡，单击“高级”

按钮。

② 在出现的高级安全设置对话框中，单击“编辑”按钮。

③ 在出现的“Windows 安全”对话框中，单击“删除”按钮。

> **提示：** 单击“复制”将会将继承下来的权限保留，你可以编辑继承下来的权限，如果点击“删除”，将会将继承下来的权限删除，你需要添加新的用户或组授权。

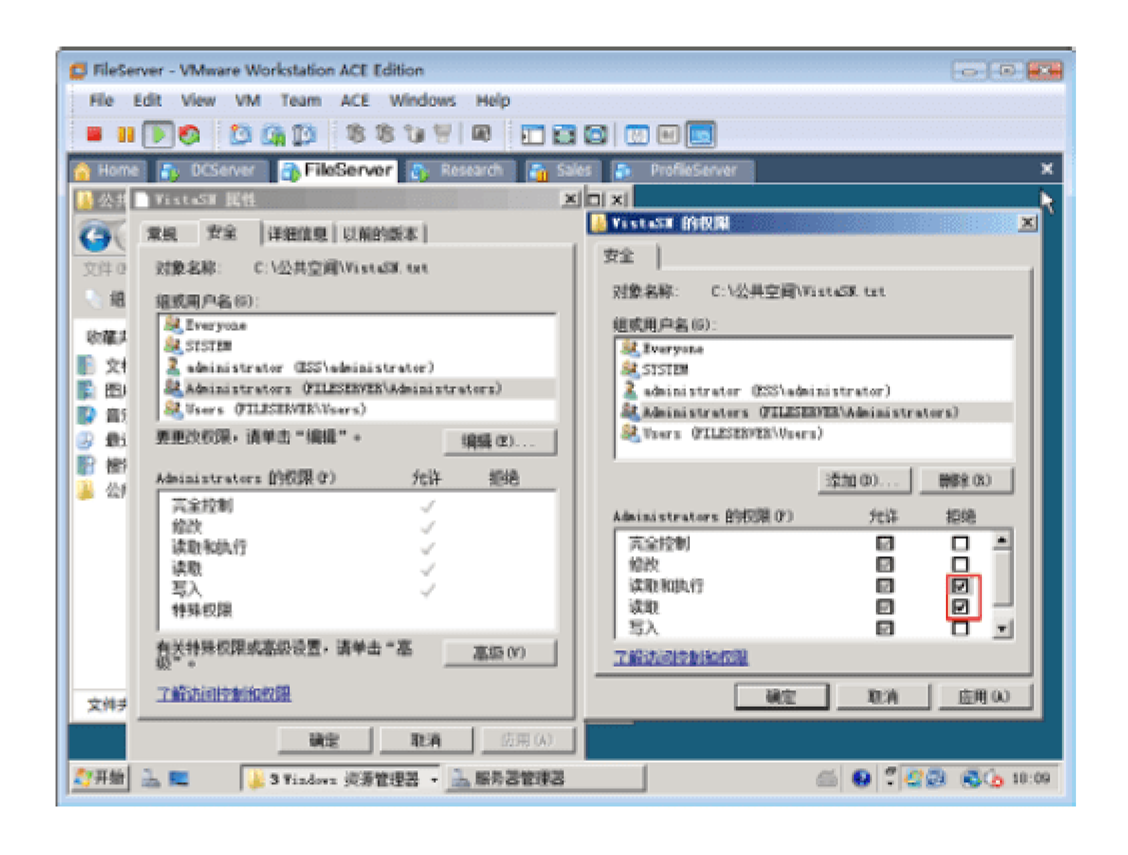


图 6-19　选择相反的权限替代继承权限

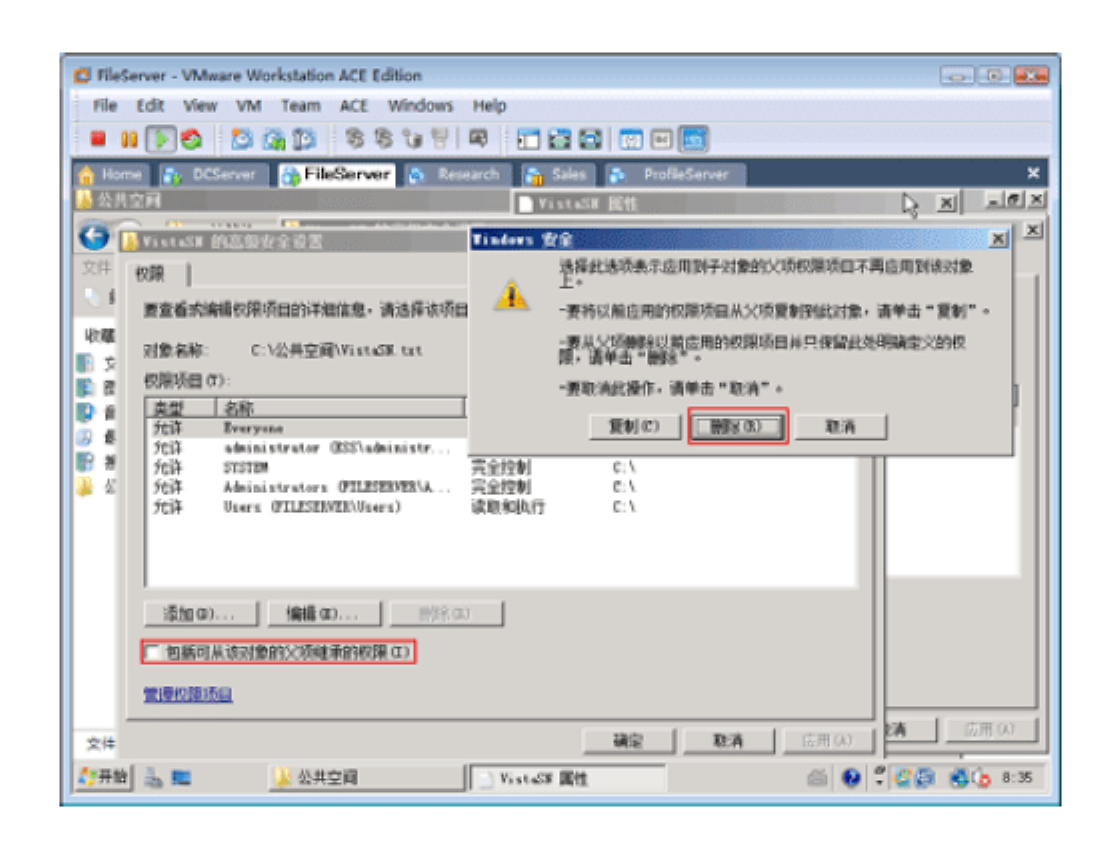


图 6-20　删除继承下来的权限

④ 如图 6-21 所示，单击“添加”按钮，输入 hanLG，单击“检查名称”按钮，单击“确定”按钮。

⑤ 如图 6-22 所示，授予韩立刚“完全控制”权限，单击“确定”按钮。现在该文件只有“韩立刚”账户能够完全控制了。

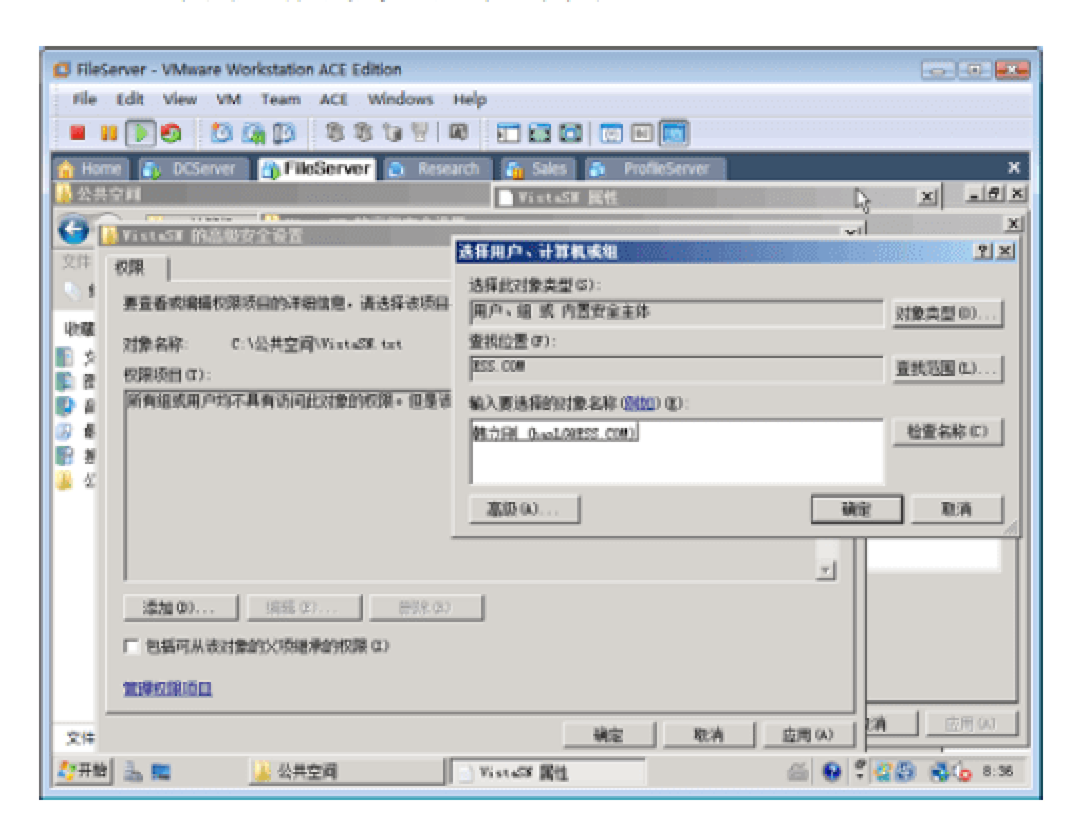


图 6-21　添加新的权限

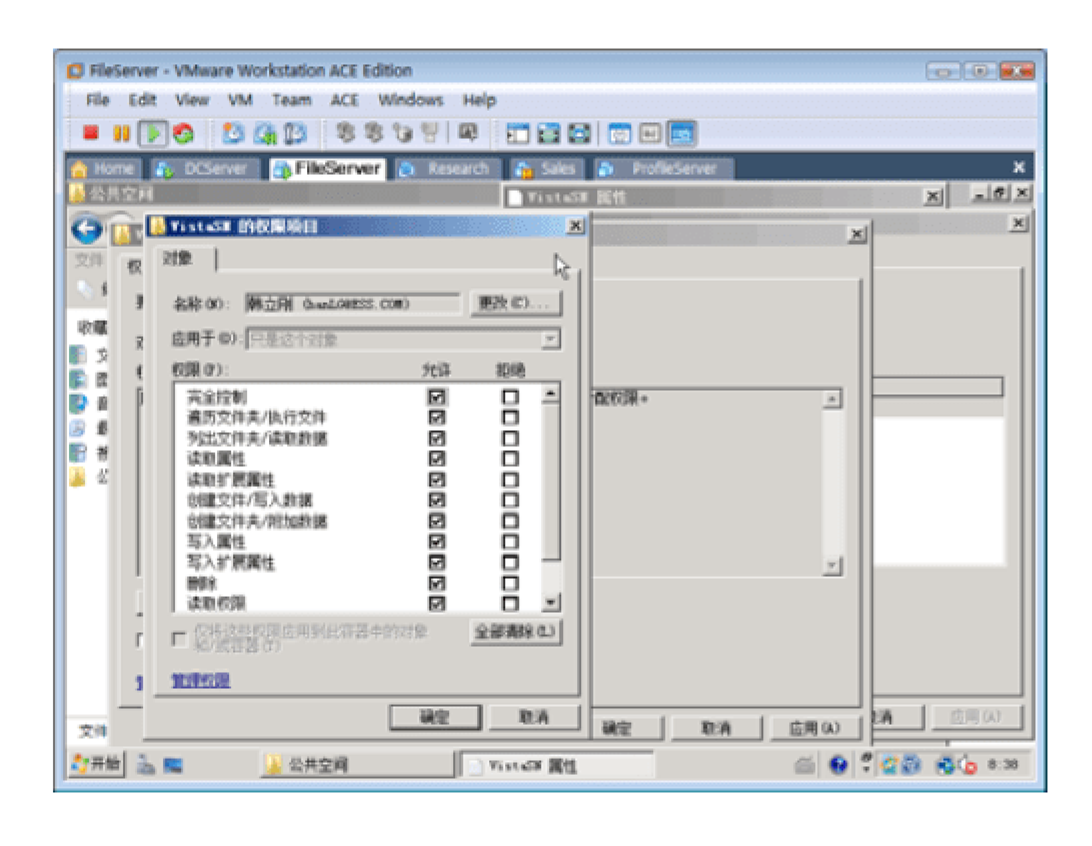


图 6-22　授予完全控制权

⑥ 此时，管理员也不能打开该记事本了。

(3) 对父文件夹进行更改，随后文件或子文件夹将继承这些权限，即更改父对象权限的应用位置。

多数情况下，除非文件夹从其父文件夹中继承冲突设置，否则“拒绝”会替代“允许”。这种情况下，从子树中最接近该对象的父文件夹继承来的设置将具有优先权。

只有可继承的权限可以由子对象继承。设置父对象的权限时，可以确定文件夹或子文件夹是否能够使用“<对象>的高级安全设置”对话框的“权限”选项卡中的“应用于”下拉列表框来继承它们。

6.3.6　重置文件的安全性

在文件夹上可以重置其内部的文件以及子文件夹的安全设置。

示例：重置安全设置。

若“公共空间”文件夹内的文件以及子文件夹的权限设置的安全性不能满足你现在的要求了，则可以重新设置“公共空间”文件夹的权限。

① 右击“公共空间”文件夹，在弹出的快捷菜单中选择“属性”命令，切换到“安全”选项卡，单击“高级”按钮。

② 在出现的高级安全设置对话框中，单击“编辑”按钮。

③ 在出现的高级安全设置对话框，如图 6-23 所示，选中“使用可从此对象继承的权限替换所有后代上现有的所有可继承权限”复选框，单击“确定”按钮。

④ 在出现的提示对话框中，单击“是”按钮。

⑤ 如图 6-24 所示，再次打开文件夹中的 VistaSN.txt，查看其安全性。发现上一节去掉的继承权限，再次被应用上，并且在上一节授权账户“韩立刚”的访问 VistaSN.txt 文件权限也不复存在了。



提示：文件以及文件夹的所有者能够无条件地设置文件的安全性，或对文件以及文件夹有完全控制权限的用户能够设置其安全性。如果里面的文件和子文件夹是其他用户账户创建的，在访问的过程中会出现权限不足的提示，则需要获得对象的所有权后，再重新设置其安全性。关于获得对象所有权，可参照 6.3.7 小节。

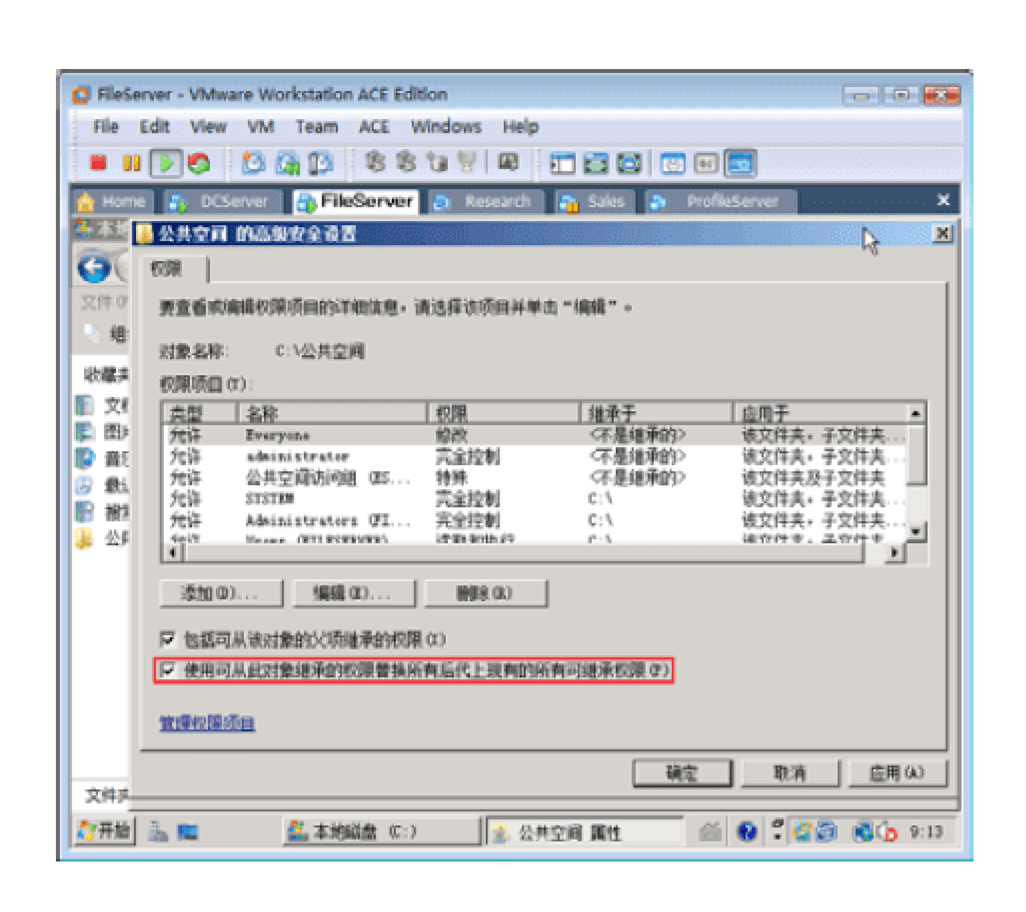


图 6-23　重置文件夹内所有对象的权限

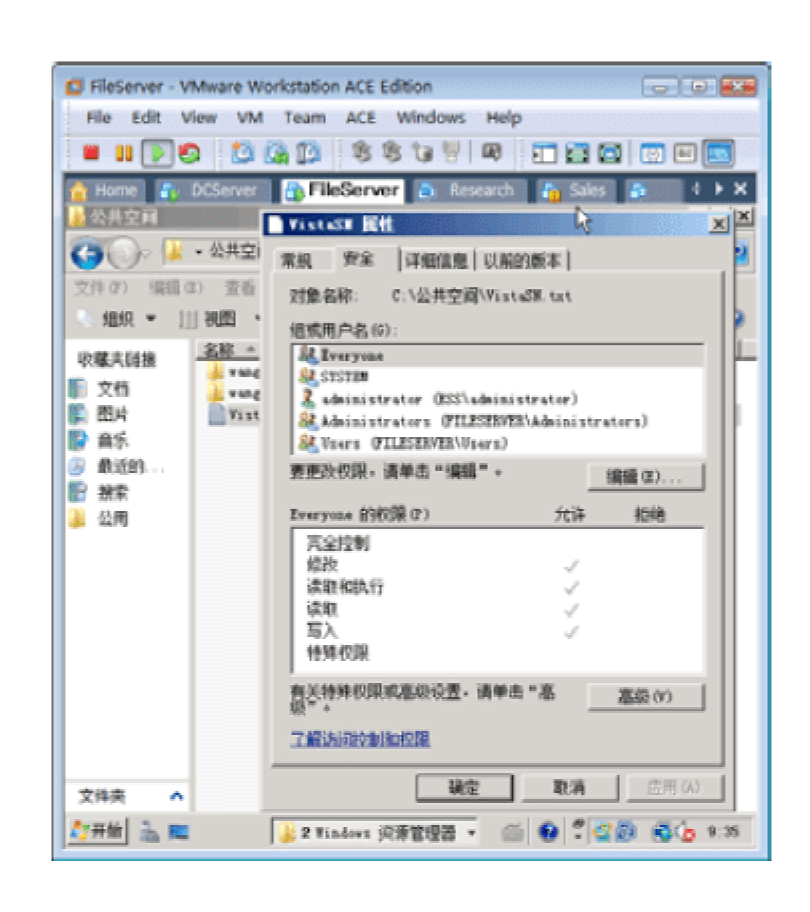


图 6-24　内部对象权限被重置

6.3.7　获得对象所有权

对象所有权

每个对象都有所有者，无论是在 NTFS 卷中或者在 Active Directory 中。所有者控制如何设置对象的权限以及将权限授予谁。

提示：需要修改或更改文件权限的管理员必须首先取得文件所有权。默认情况下，所有者是创建对象的实体。所有者可始终更改对象的权限，即使已经拒绝了到对象的所有访问。

如下人员可以取得所有权。

- 管理员。默认情况下，Administrators 组拥有“取得文件或其他对象的所有权”用户权利。
- 具有对相关对象的“取得所有权”权限的任何人或任何组。
- 拥有“存储文件和目录”用户权利的用户。

所有权可以用以下方式转换。

- 当前的所有者可以向其他用户授予“取得所有权”权限，允许该用户随时取得所有权。该用户必须实际取得所有权才能完成所有权的转移。
- 管理员可以取得所有权。
- 拥有“存储文件和目录”用户权利的用户可以双击“其他用户和组”并选择任意用户或组来向其分配所有权。

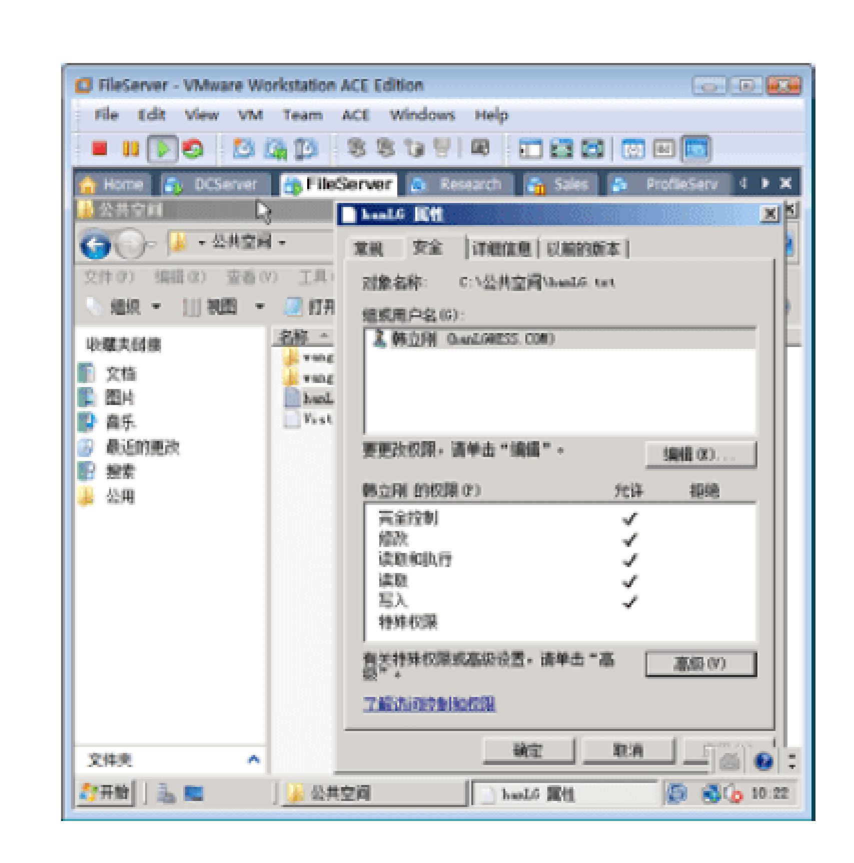


图 6-25　更改 NTFS 权限

示例 1：管理员获得对象的所有权。

① 以“韩立刚”用户账户登录 FileServer，在公共空间创建一个文件 hanLG.txt，阻断继承的权限，授予自己能够完全控制，如图 6-25 所示。

② 打开高级安全设置对话框，查看记事本的所有者，如图 6-26 所示。



提示：该记事本只有“韩立刚”用户账号能够访问，所有者默认就是创建者。管理员组的用户创建的对象，所有者默认是管理员组的所有成员。

③ 以管理员的身份登录，双击打开该记事本文件，提示拒绝访问。

④ 打开 hanLG.txt 记事本文件属性，切换到“安全”选项卡，单击“继续”按钮，如图 6-27 所示。

⑤ 如图 6-28 所示，在出现的高级安全设置对话框中，看不到所有者。

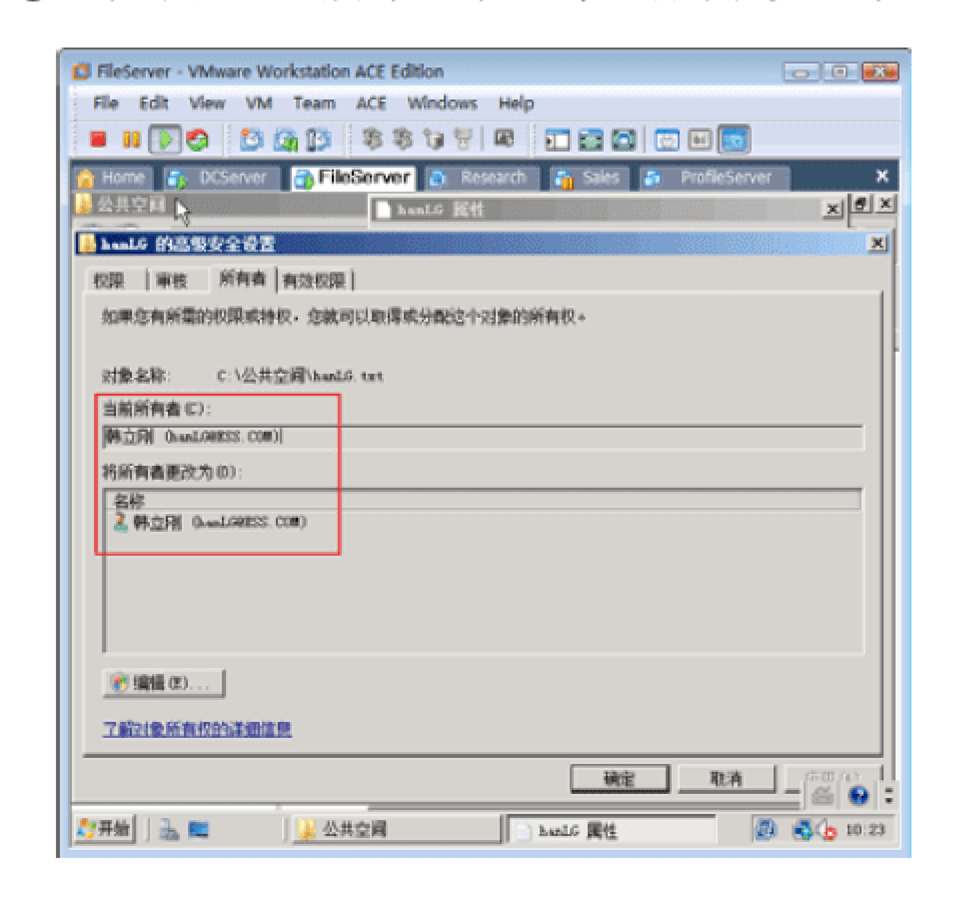


图 6-26　查看所有者

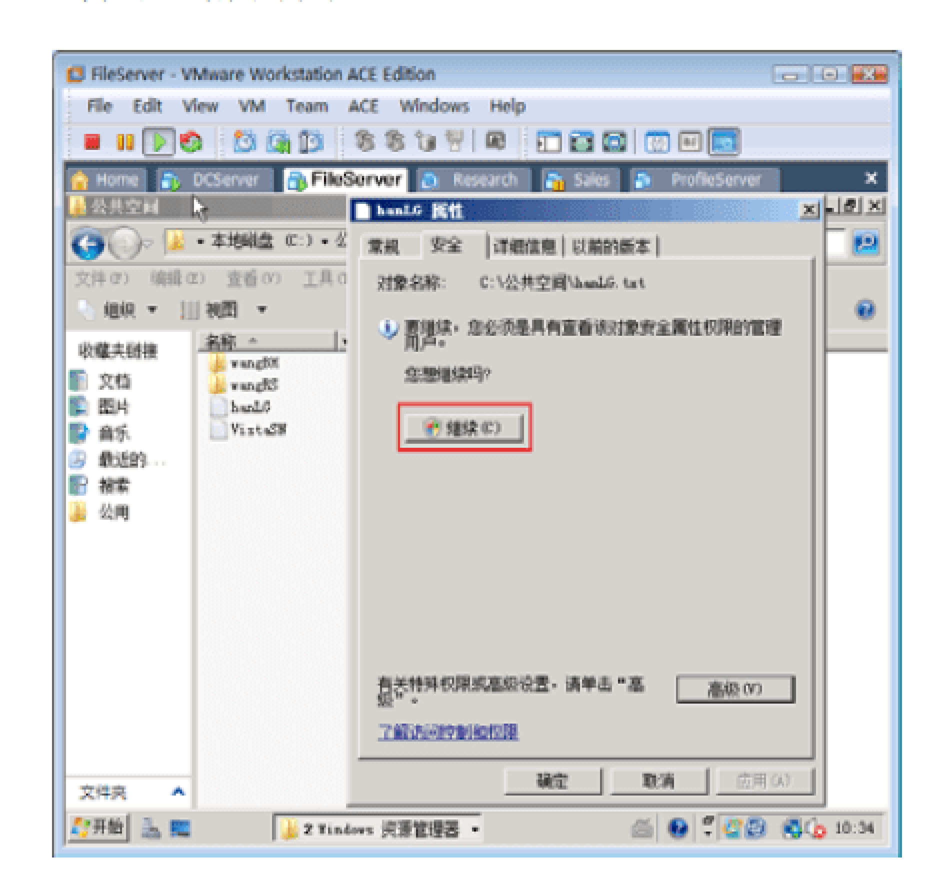


图 6-27　查看安全设置

⑥ 如图 6-28 所示，选中 administrator 账户，单击“确定”按钮，在出现的提示对话框中，单击“确定”按钮。关闭对话框。

⑦ 再次打开 hanLG.txt 记事本文件属性对话框，如图 6-29 所示，此时可以编辑其权限了，因为所有者已经是管理员了。

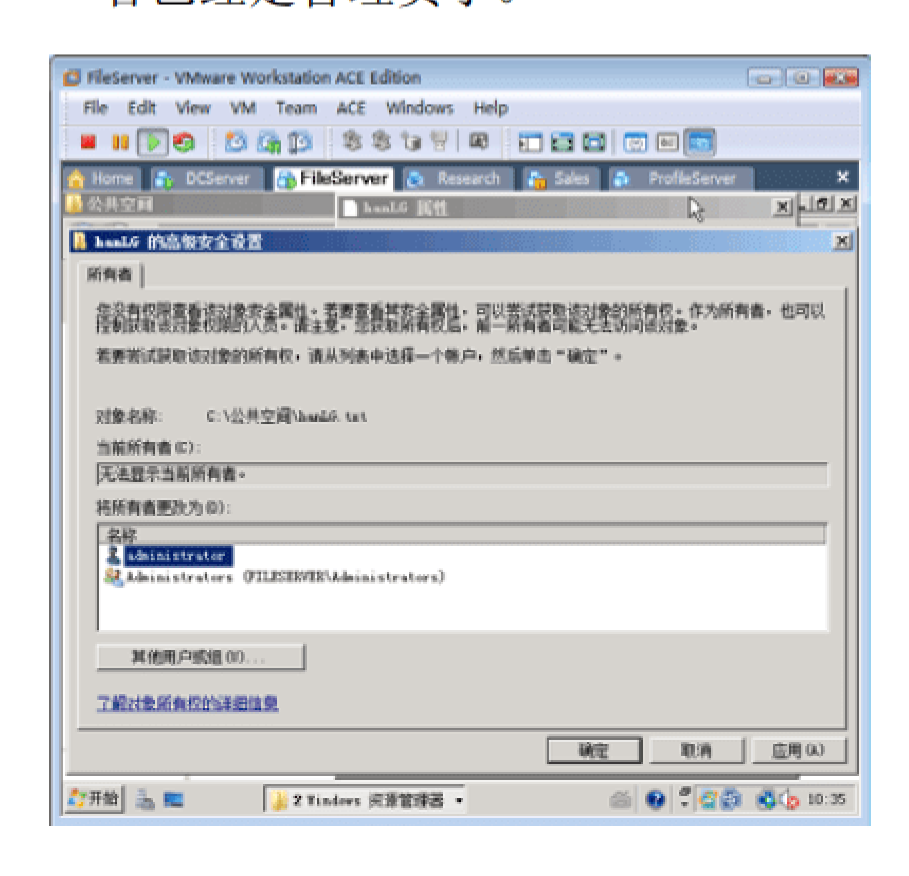




图 6-28　获得所有权

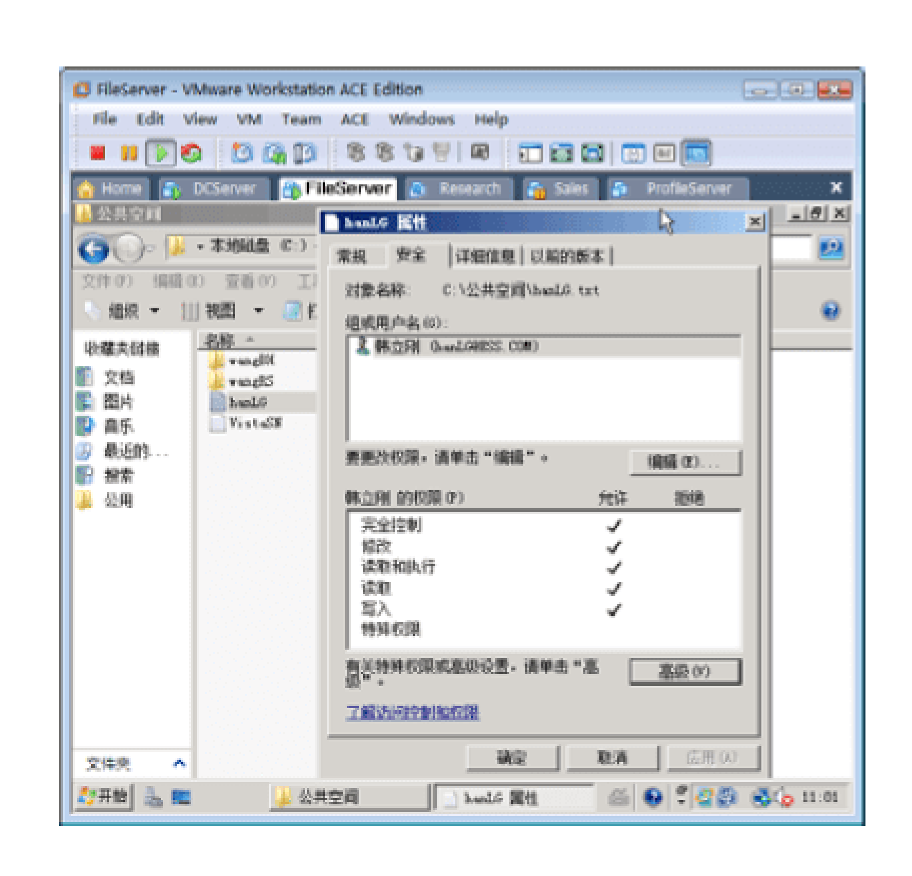


图 6-29　可以看到权限

示例 2： 更改文件夹以及其内的所有对象的所有权。

① 打开“公共空间”文件夹高级安全属性，如图 6-30 所示，切换到“所有者”选项卡，单击“编辑”按钮。

② 如图 6-31 所示，选中“替换子容器和对象的所有者”复选框，单击“确定”按钮。

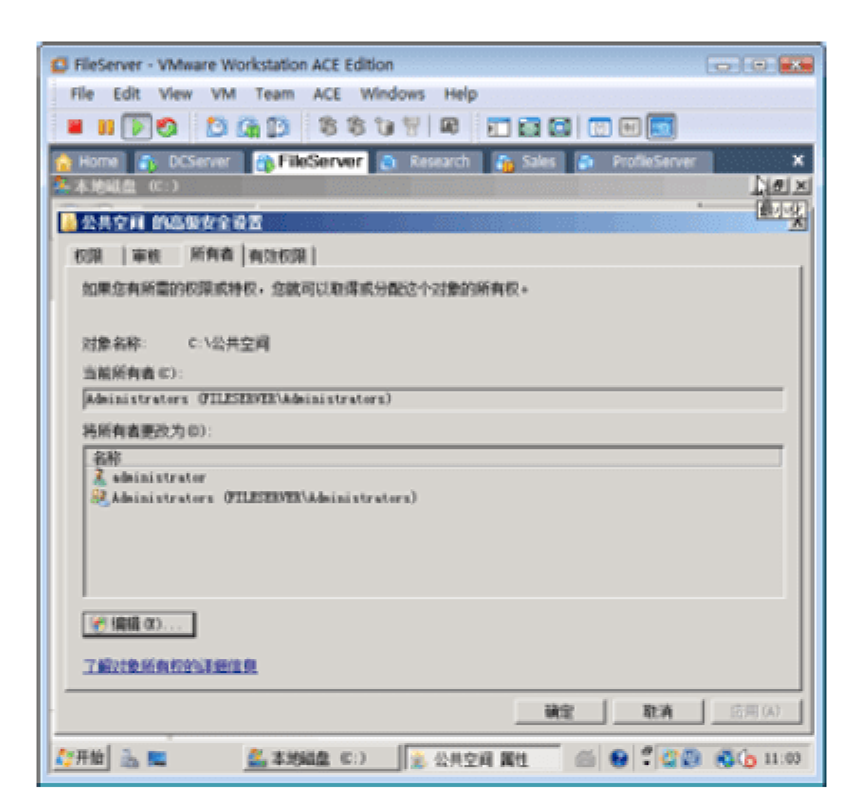


图 6-30　查看文件夹的所有者

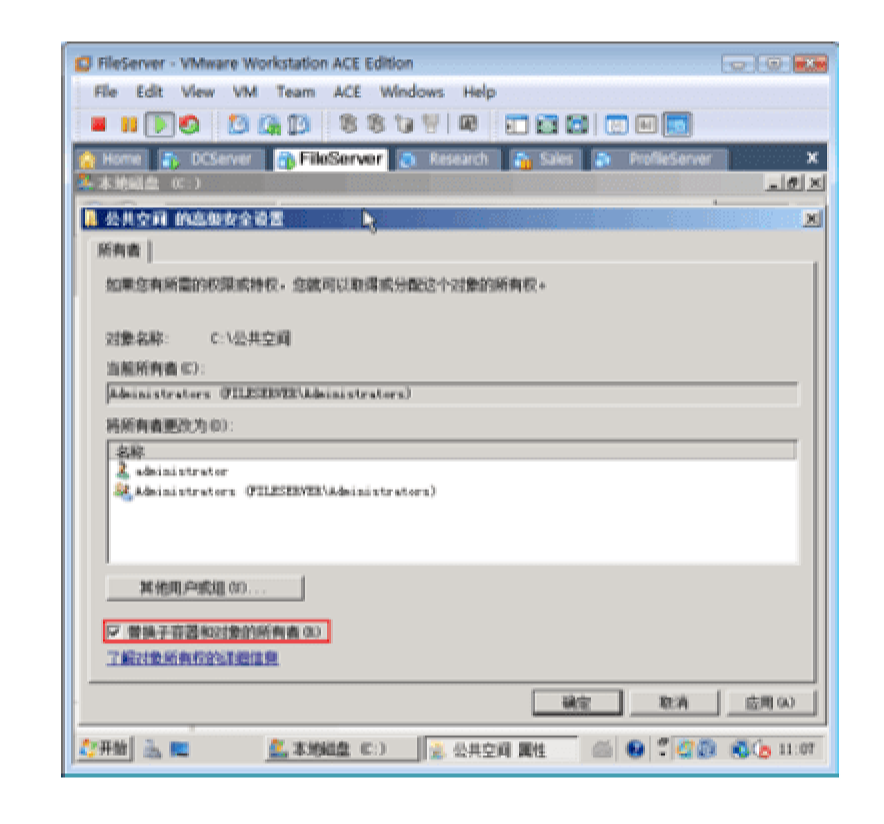
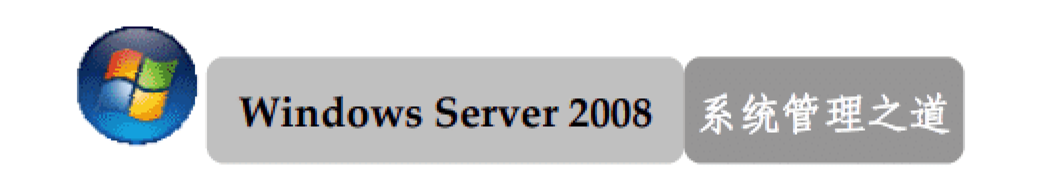


图 6-31　替换子容器和对象的所有者

6.3.8　确定对象的有效权限

每个对象都有与其相关联的一组有效权限。“高级安全设置”属性的“有效权限”选项区中列出了那些将通过组成员身份直接授权的选定组或基于用户授权访问的权限。如果要查找用户或组对于对象具有哪些权限，可以使用有效权限工具。

有效权限工具可以计算指定用户或组授予的权限。计算时，将会考虑组成员身份生效的权限，以及从



父对象继承的任何权限。另外，还会查找用户或组作为其成员的所有域和本地组。

用于确定有效权限的因素如下：

- 全局组成员身份。
- 本地组成员身份。
- 本地权限。
- 本地特权。
- 通用组成员身份。

示例：确定对象的有效权限。

① 右击“公共空间”文件夹，在弹出的快捷菜单中选择“属性”命令，切换到“安全”选项卡。

② 如图 6-32 所示，单击“高级”按钮。在出现的高级安全对话框中，切换到“有效权限”选项卡，单击“选择”按钮。

③ 如图 6-33 所示，在“选中用户、计算机和组”对话框中，输入“韩立刚”，单击“检查姓名”按钮，然后单击“确定”按钮。

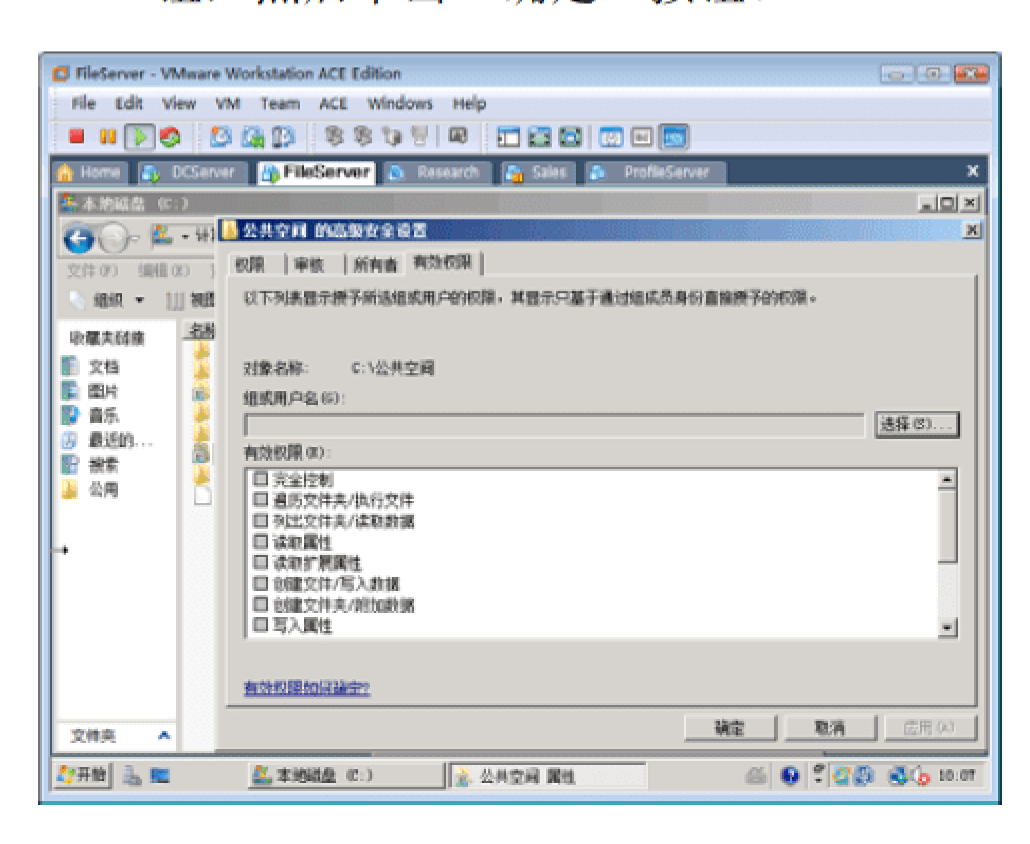



图 6-32　确定用户有效权限

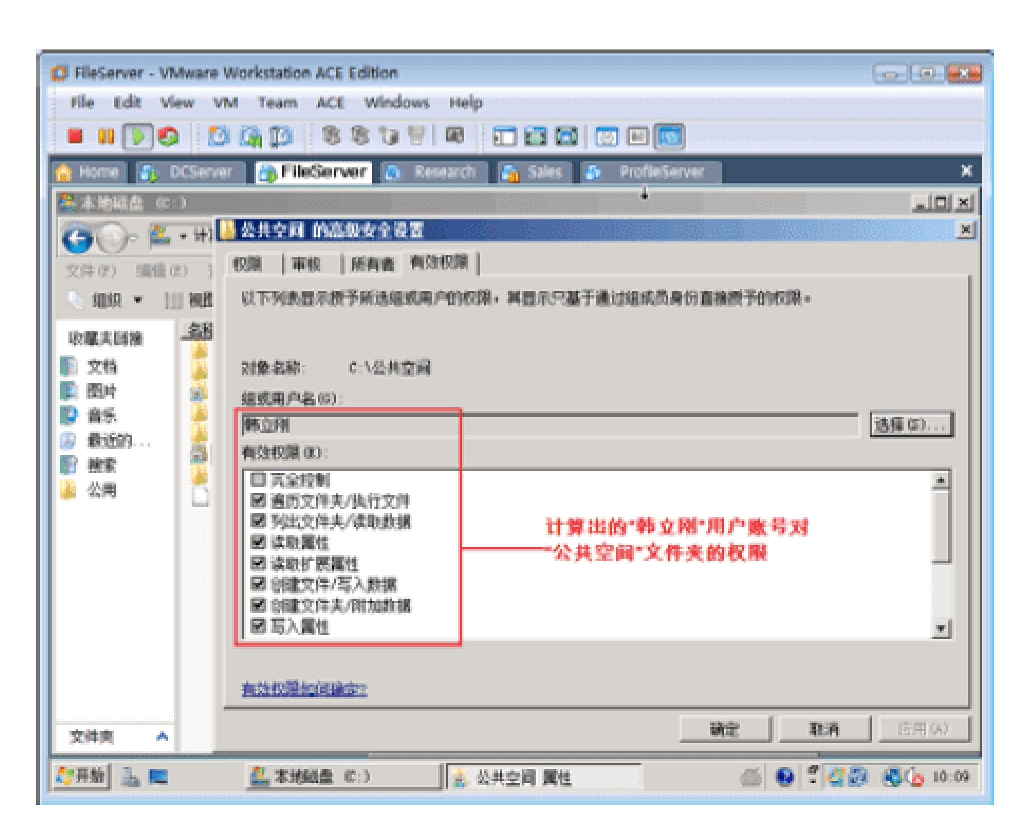


图 6-33　选择用户查看有效权限

6.3.9　保护具有 NTFS 权限的文件的最佳操作

设置 NTFS 权限时应遵循以下最佳操作。

- 将权限指派给组而不是用户。由于直接维护用户账户效率不高，因此最好不要将权限直接指派给用户。
- 如果可能，避免更改文件系统对象的默认权限项，尤其是系统文件夹和根文件夹。更改默认权限可能会出现意外的访问问题或者降低安全性。
- 不拒绝 Everyone 组访问某个对象。如果拒绝 Everyone 访问某个对象，则管理员也不能访问该对象。更好的解决方案是删除 Everyone 组，只要给其他用户、组或计算机授予访问该对象的权限即可。此外，可能需要为 Administrators 组和 LocalSystem 指派“完全控制”权限。
- 如果对象具有显式允许权限，则继承的拒绝权限并不禁止访问该对象。显式权限优于继承的权限，其中包括继承的拒绝权限。
- 拒绝权限只能用于以下特殊情形。

  - 从具有“允许”权限的组中排除部分成员。
  - 为用户或组指派“完全控制”权限后排除一个特殊的权限。
- 为网站配置 NTFS 权限时应小心使用。权限设置不当可能会拒绝有效用户访问需要的文件和目录。例如，即使用户有查看和执行程序的正确权限，而可能还是无权访问运行该程序所需的特定动态链接库(DLL)。要保证用户可以安全和不间断地访问文件，可将相关文件放在同一目录下，并为该目录指派相应的 NTFS 权限。

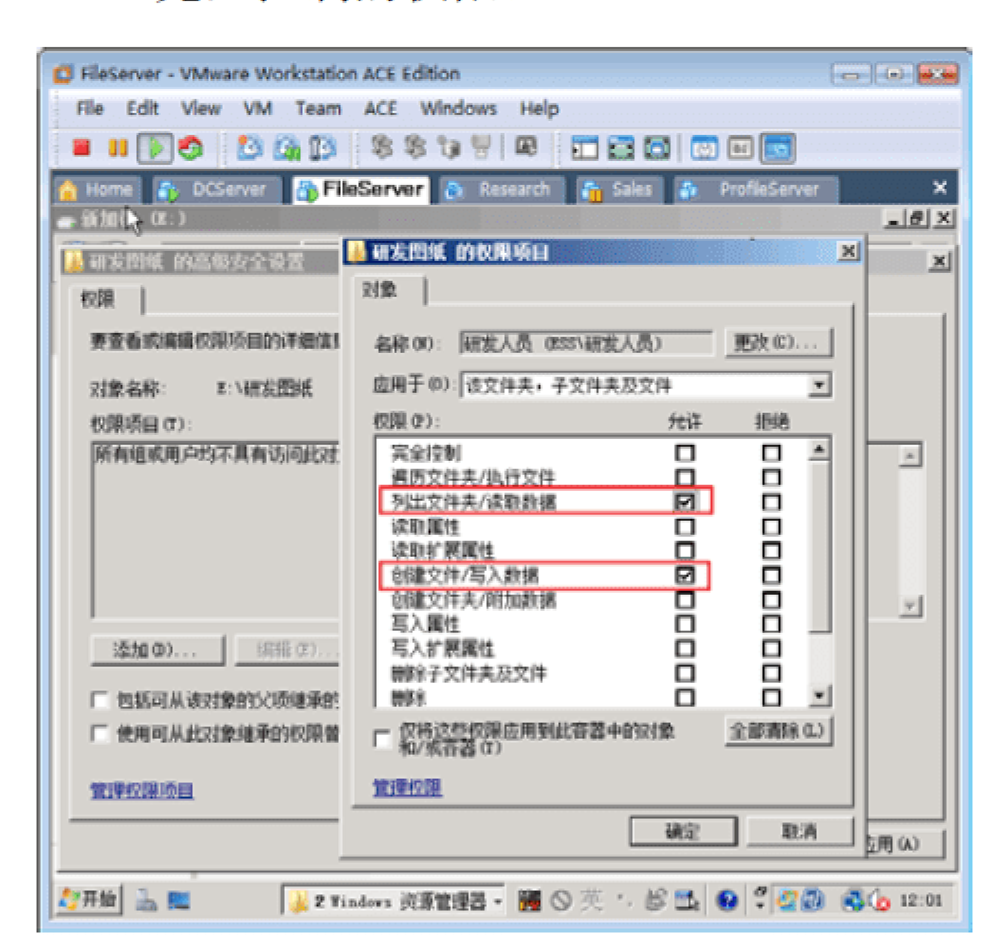
6.3.10　NTFS 权限应用实战

1. 场景一

研发部经理打算实现这样的功能：员工制作的图纸一旦提交之后就不允许员工再访问，防止员工不小心删除，由归档员“兰帅”来处理提交的图纸。

① 创建一个“研发图纸”文件夹，在“研发图纸”高级安全对话框中，取消选中“包括可从该对象的父项继承的权限”复选框。在弹出的对话框中，单击“删除”按钮。单击高级安全对话框中的“添加”按钮，输入“研发人员”，单击“检查名称”，单击“确定”按钮。如图 6-34 所示，授予研发人员“列出文件夹/读取数据”和“创建文件/写入数据”的权限。单击“确定”按钮。

② 再次单击“添加”按钮，输入“兰帅”，单击“检查名称”按钮，如图 6-35 所示，授予“兰帅”完全控制的权限。



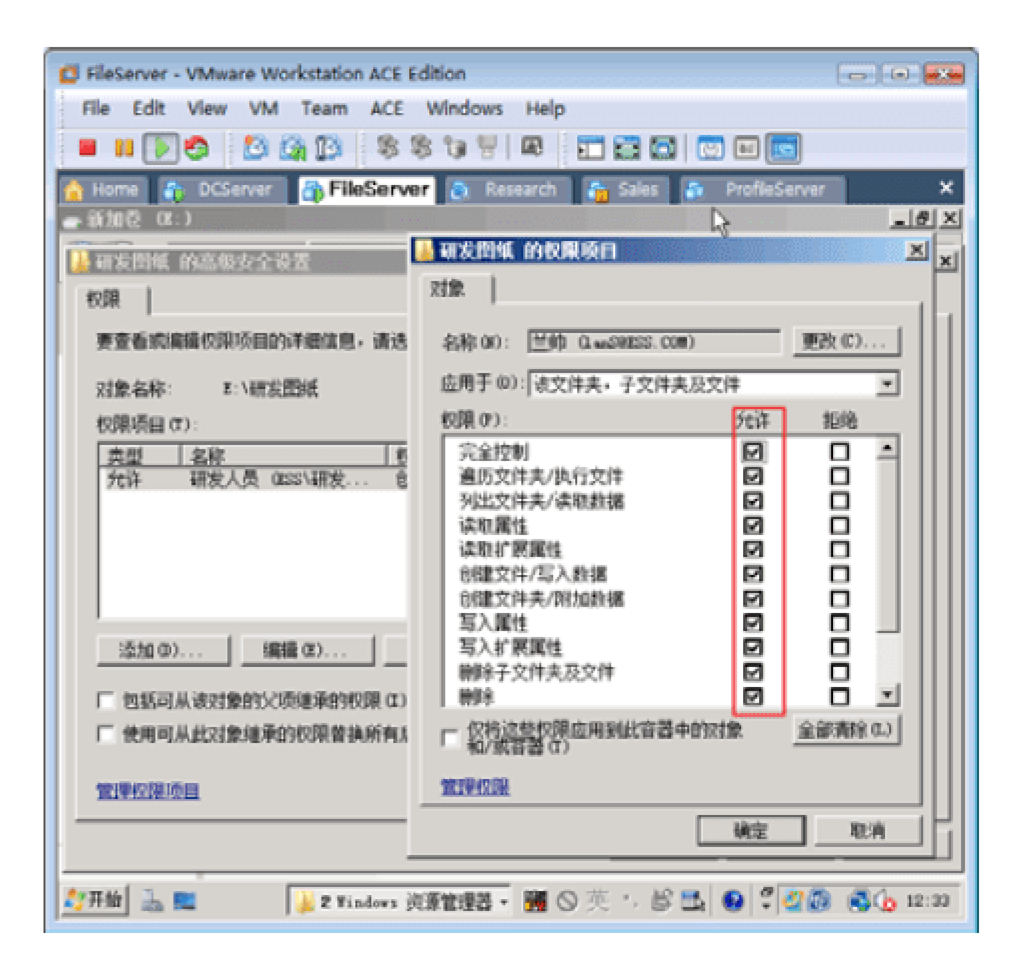




图 6-34　设置权限

图 6-35　授予完全控制权限

2. 场景二

“公共空间”文件夹，存储所有用户的数据，为了管理方便，不允许用户随便在“公共空间”文件夹中创建文件和文件夹，管理员为每个用户创建一个文件夹，并授予用户对自己文件夹的完全控制权。

① 如图 6-36 所示，打开“公共空间”文件夹安全属性，去掉继承下来的权限，授予管理员完全控制的权限，授予 Domain Users 列出文件夹/读取数据的权限。

② 在“公共空间”文件夹，为每个用户创建子文件夹，如图 6-37 所示，单击“高级”按钮，打开高级安全设置对话框，单击“添加”按钮授予“韩立刚”账户完全控制权。单击“确定”按钮。

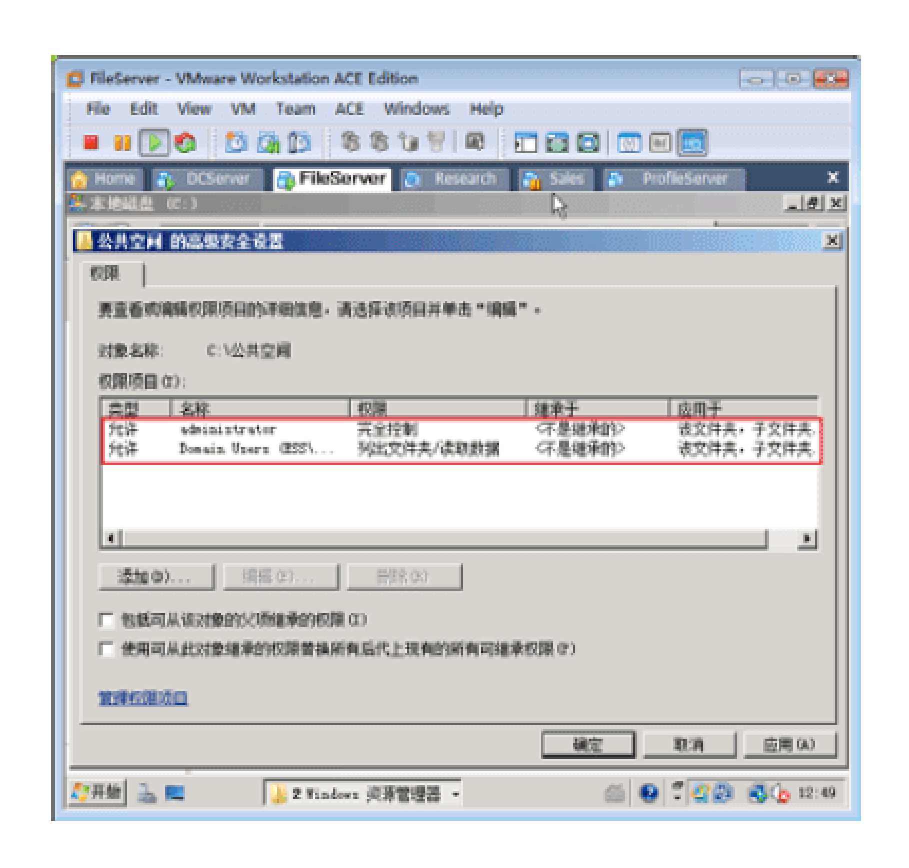


图 6-36 更改文件夹的权限

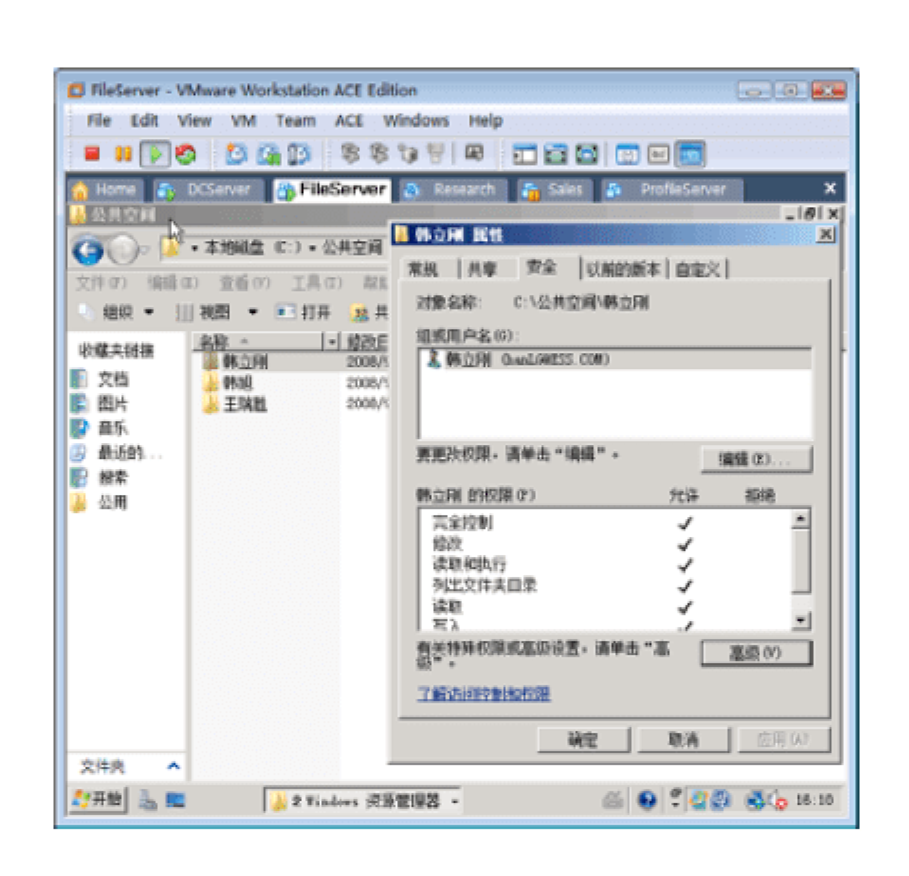


图 6-37 针对每个用户的文件夹单独授权

6.4 加密文件系统

EFS(Encrypting File System，加密文件系统)是 Windows 2000/XP/Vista/Server 2008 所特有的一个实用功能，加密文件系统 (EFS) 提供了用于在 NTFS 文件系统卷上存储加密文件的核心文件加密技术。由于 EFS 与文件系统相集成，因此使管理更方便，使系统难以被攻击，并且对用户是透明的。此技术对于保护计算上可能易被其他用户访问的数据特别有用。对文件或文件夹加密后，即可像使用任何其他文件和文件夹那样，使用加密的文件和文件夹。

EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的 FEK(File Encryption Key，文件加密钥匙)，然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。随后系统利用用户的公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密 FEK，然后利用 FEK 解密出文件。在首次使用 EFS 时，如果用户还没有公钥/私钥对(统称为密钥)，则会首先生成密钥，然后加密数据。如果你登录到了域环境中，密钥的生成依赖于域控制器，否则依赖于本地机器。

EFS 加密系统对用户是透明的。这也就是说，如果你加密了一些数据，那么你对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问加密过的数据时，将会收到“访问拒绝”的错误提示。EFS 加密的用户验证过程是在登录 Windows 时进行的，只要登录到 Windows，就可以打开任何一个被授权的加密文件。

6.4.1 EFS 加密

选中 NTFS 分区中的一个文件后右击，在弹出的快捷菜单中选择“属性”命令，在随后出现的对话框中，切换到“常规”选项卡。然后单击“高级”按钮，在出现的对话框中选中“加密内容以便保护数据”复选框，单击“确定”按钮即可。

此时你会发现，加密文件名的颜色变成了绿色。当其他用户登录系统后打开该文件时，就会出现“拒绝访问”的提示，这表示 EFS 加密成功。而如果想取消该文件的加密，只需取消选中“加密内容以便保护数据”复选框即可。

示例：EFS 加密。

① 以域用户“韩立刚”登录到 Research 计算机上。

② 如图 6-38 所示，右击桌面上的 IE 图标，在弹出的快捷菜单中选择“属性”命令，在 IE 属性对话框中，切换到“内容”选项卡，单击“证书”按钮。

③ 如图 6-39 所示，打开“证书”对话框。此时可以看到没有任何个人证书。

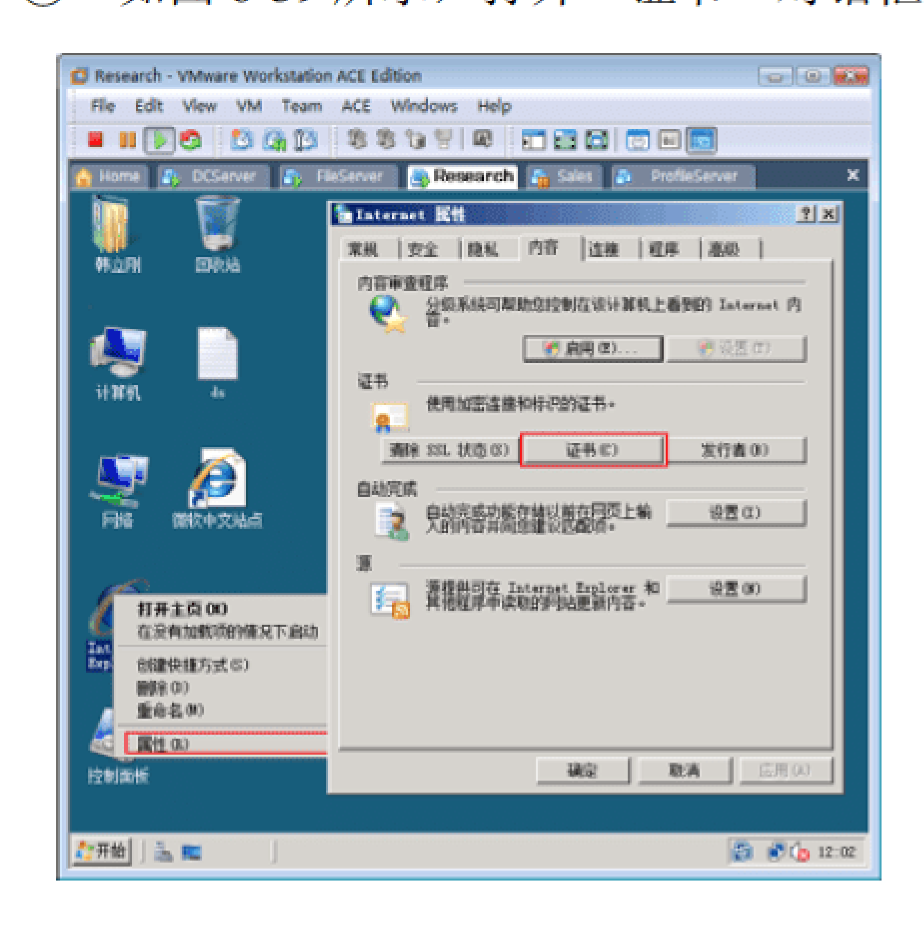




图 6-38　查看用户的证书

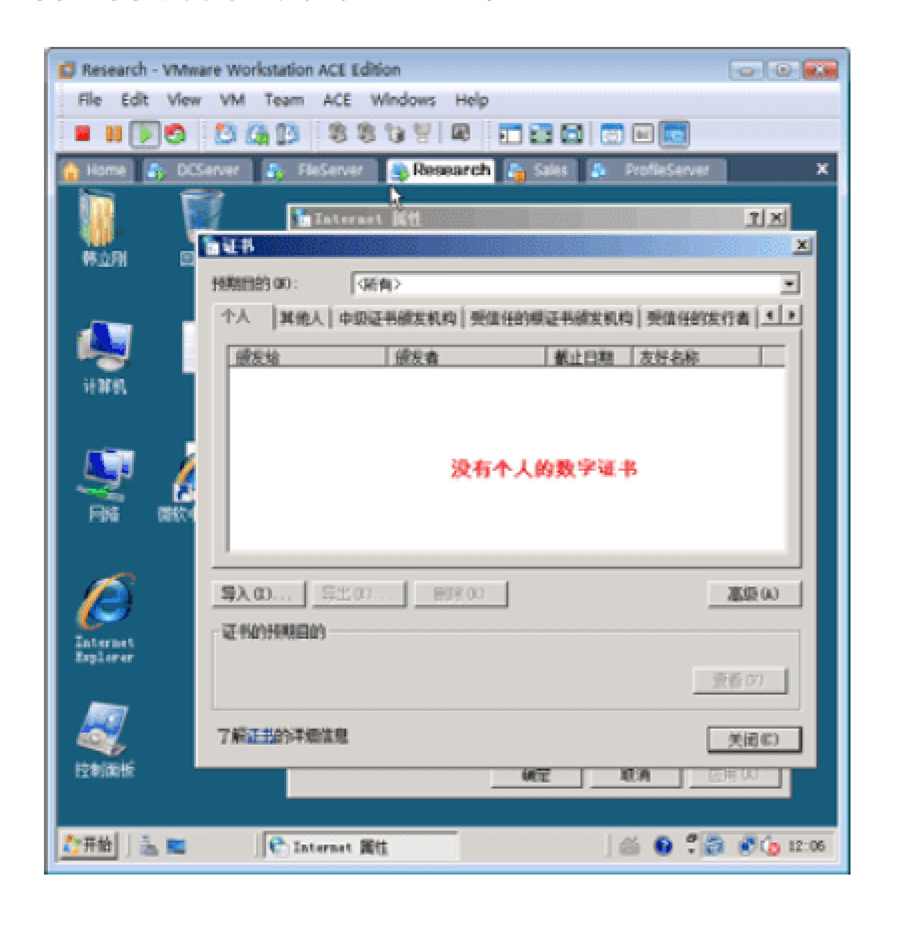


图 6-39　查看个人证书

注意：EFS 使用加密密钥对数据进行加密。加密密钥与证书绑定在一起。首次加密文件或文件夹时，将为用户创建加密证书和密钥。

④ 在 E 盘上创建一个文件夹 hanLG EFS，右击该文件夹，在弹出的快捷菜单中选择“属性”命令。

⑤ 在“常规”选项卡中，单击“高级”按钮。在高级属性对话框中，如图 6-40 所示，选中“加密内容以便保护数据”复选框，单击“确定”按钮。此时，你将发现加密后的文件夹变成了绿色。

⑥ 再次打开 IE 属性对话框，在“内容”选项卡中，单击“证书”按钮，如图 6-41 所示，可以看到当前用户用于 EFS 的数字证书。选中 hanLG 证书，单击“查看”按钮。

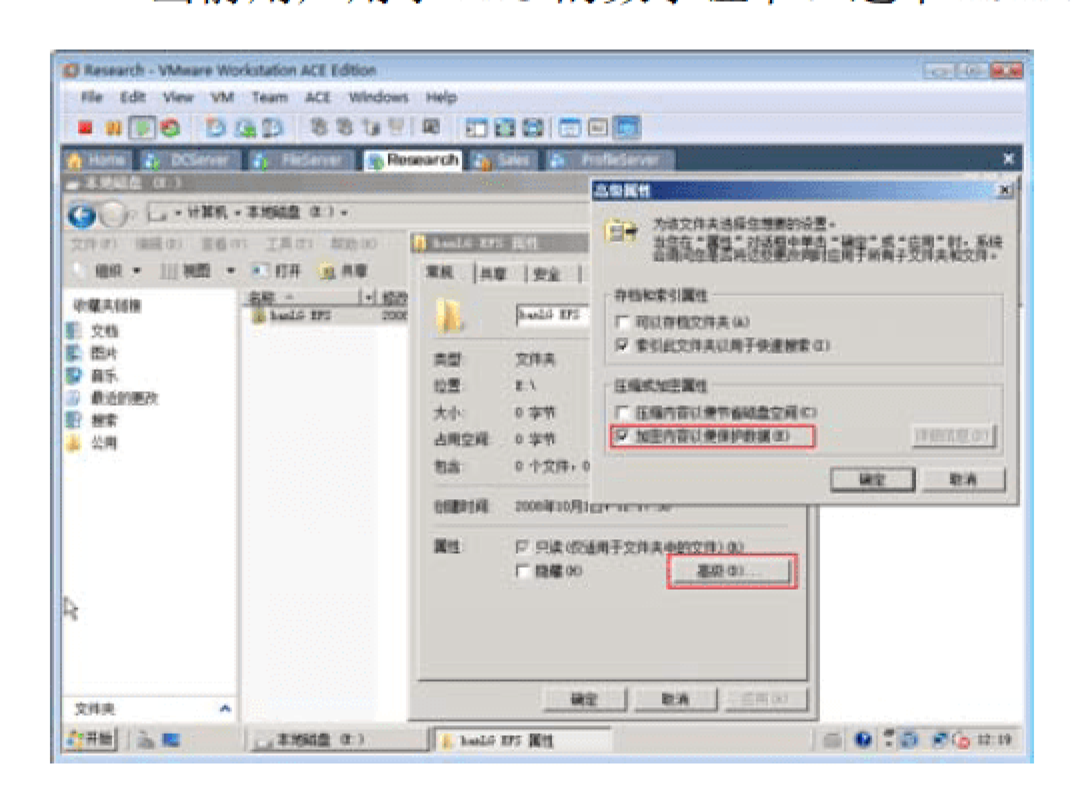


图 6-40　加密文件夹

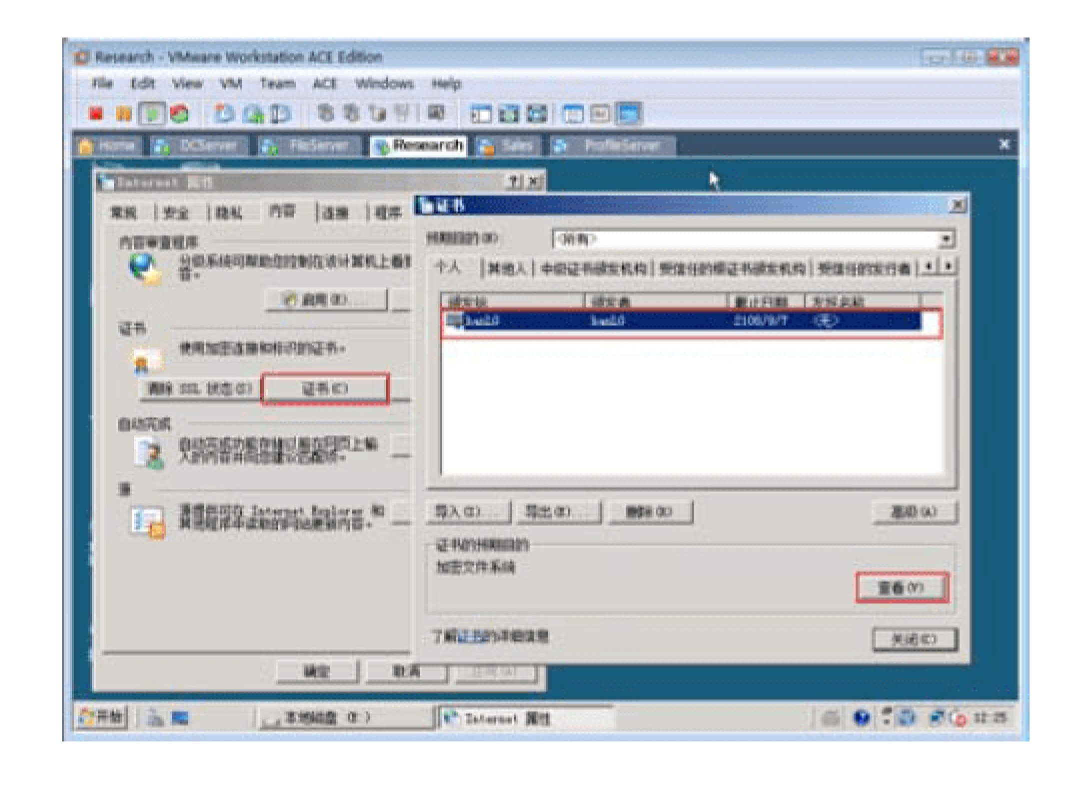


图 6-41　查看系统分配给用户的证书

⑦ 如图 6-42 所示，可以看到证书的信息。

⑧ 在 hanLG EFS 文件夹中创建一个记事本文件 hanLG Test.txt，你会发现该记事本文件自动被加密。

⑨ 换一个域账户“韩旭”登录到 Research 计算机。发现不能访问“韩立刚”加密的文件 hanLG Test.txt。

注意：这里出现的拒绝访问，不是 NTFS 权限拒绝访问，而是因为韩旭账户不能解密韩立刚账户加密的文件。

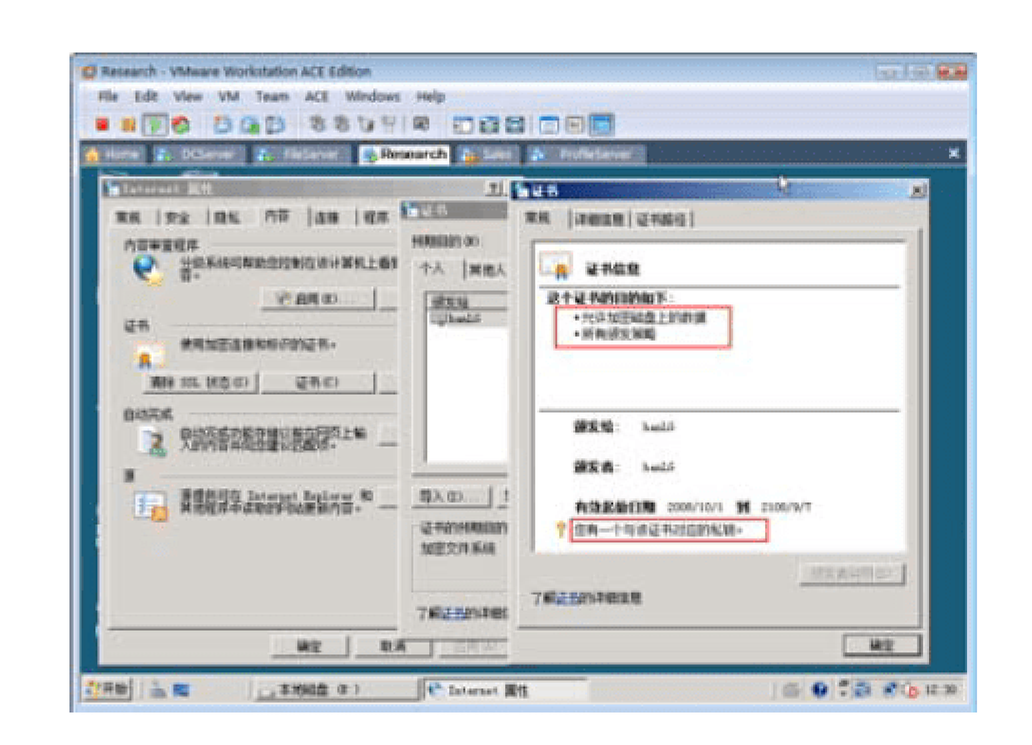


图 6-42 查看证书详细信息

6.4.2 备份 EFS 证书

如果其他人想共享经过 EFS 加密的文件或文件夹，又该怎么办呢？由于重装系统后，SID(安全标识符)的改变会使原来由 EFS 加密的文件无法打开，所以为了保证别人能共享 EFS 加密文件或者重装系统后可以打开 EFS 加密文件，必须备份证书。

备份 EFS 证书的几种方式如下。

1. 通过 IE 属性备份 EFS 证书

① 打开 IE 属性对话框，切换到“内容”选项卡，单击“证书”按钮。

② 如图 6-43 所示，选中要导出的证书，单击“导出”按钮。在出现的“证书导出向导”对话框中，单击“下一步”按钮。

③ 如图 6-44 所示，在出现的“导出私钥”设置界面中，选中“是，导出私钥”单选按钮，单击“下一步”按钮。

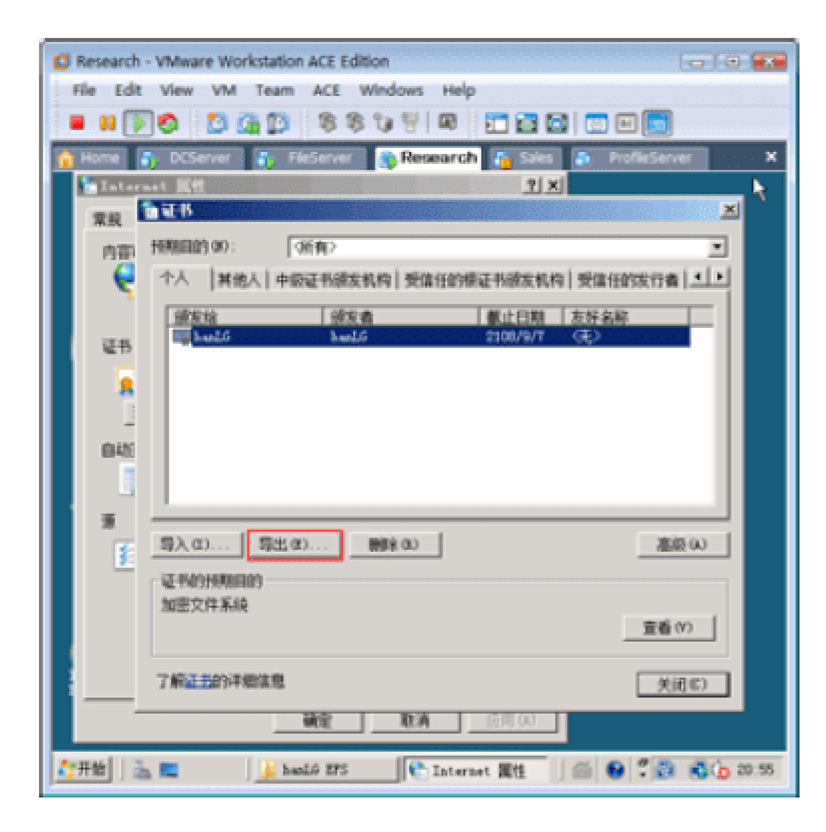


图 6-43 导出数字证书

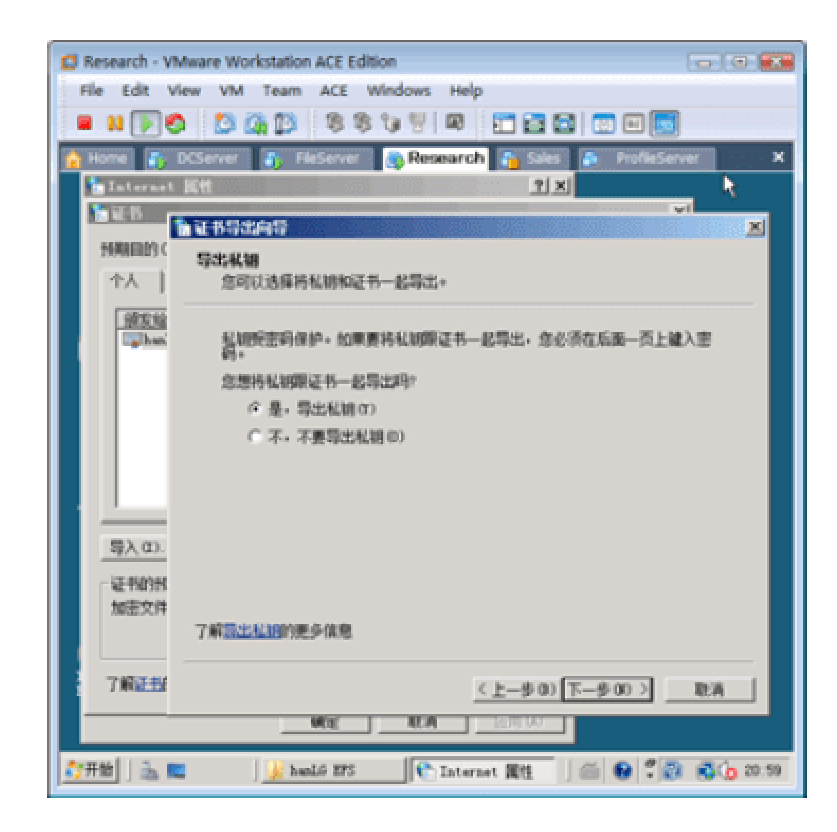


图 6-44 选择导出私钥

④　如图 6-45 所示，在出现的“导出文件格式”界面中，单击“下一步”按钮。

⑤　如图 6-46 所示，输入密码保护私钥，单击“下一步”按钮。



注意：该密码要牢记，以后导入该数字证书时需要用到该密码。

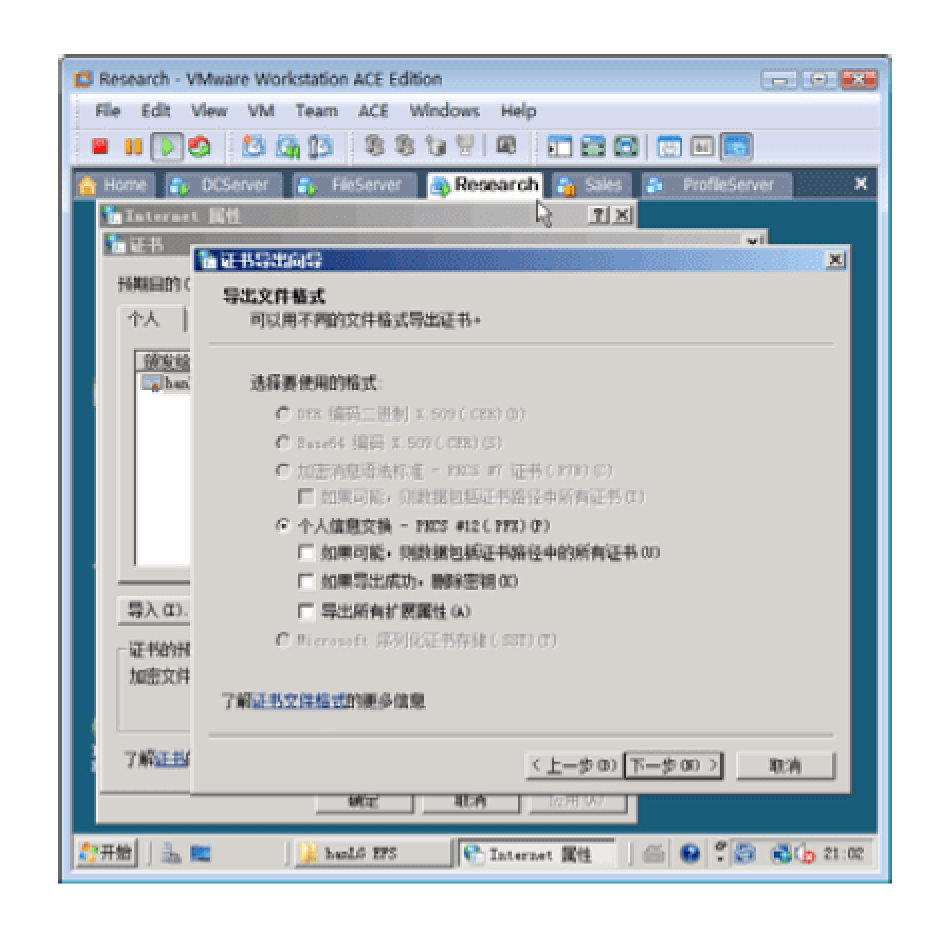


图 6-45　选择导出格式

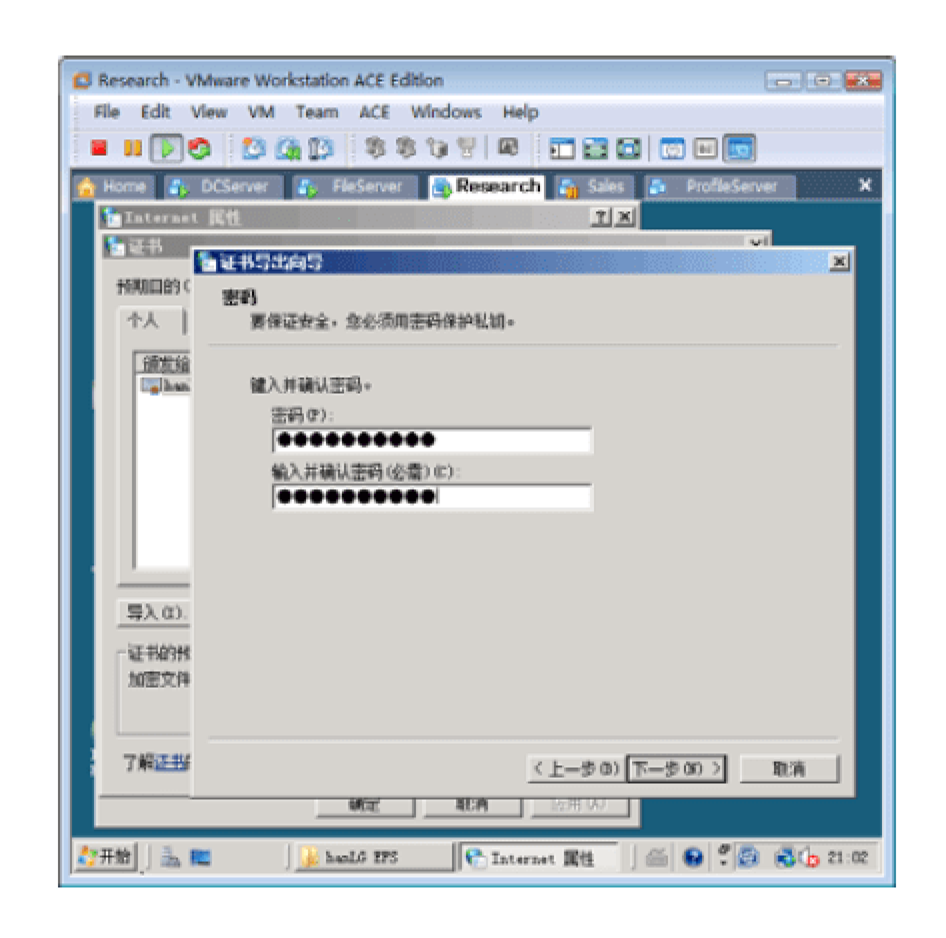


图 6-46　输入密码

⑥　如图 6-47 所示，输入证书的存储位置和文件名，完成证书导出向导。

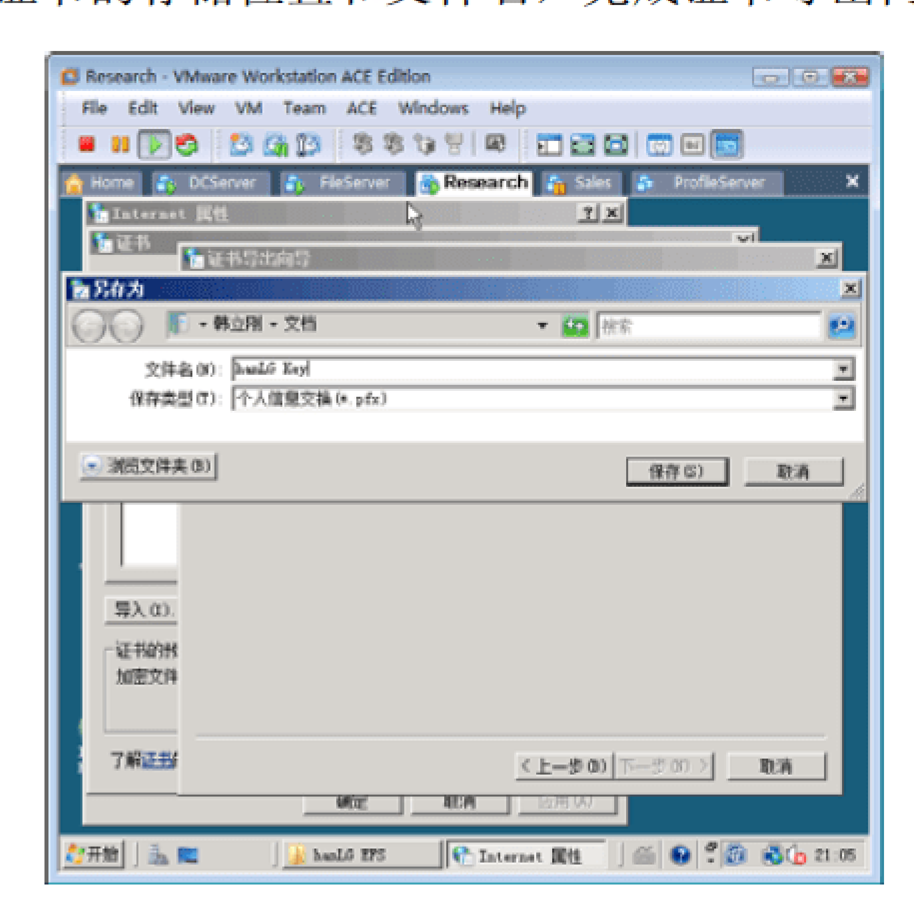


图 6-47　输入导出的证书名称

2. 通过“用户账户”备份属性

①　选择“开始”→“设置”→“控制面板”→“用户账户”命令，如图 6-48 所示，单击“管理您的文件加密证书”选项。

②　如图 6-49 所示，在出现的“管理文件加密证书”向导中，单击“下一步”按钮。

③　打开如图 6-50 所示的对话框，选择 EFS 加密使用的数字证书，单击“下一步”按钮。

④　如图 6-51 所示，输入备份的位置和密钥，单击“下一步”按钮。

⑤　如图 6-52 所示，更新以前加密的文件，选中加密的目录，单击“下一步”按钮。

⑥　如图 6-53 所示，单击“关闭”按钮，完成证书备份向导。



图 6-48　管理您的文件加密证书

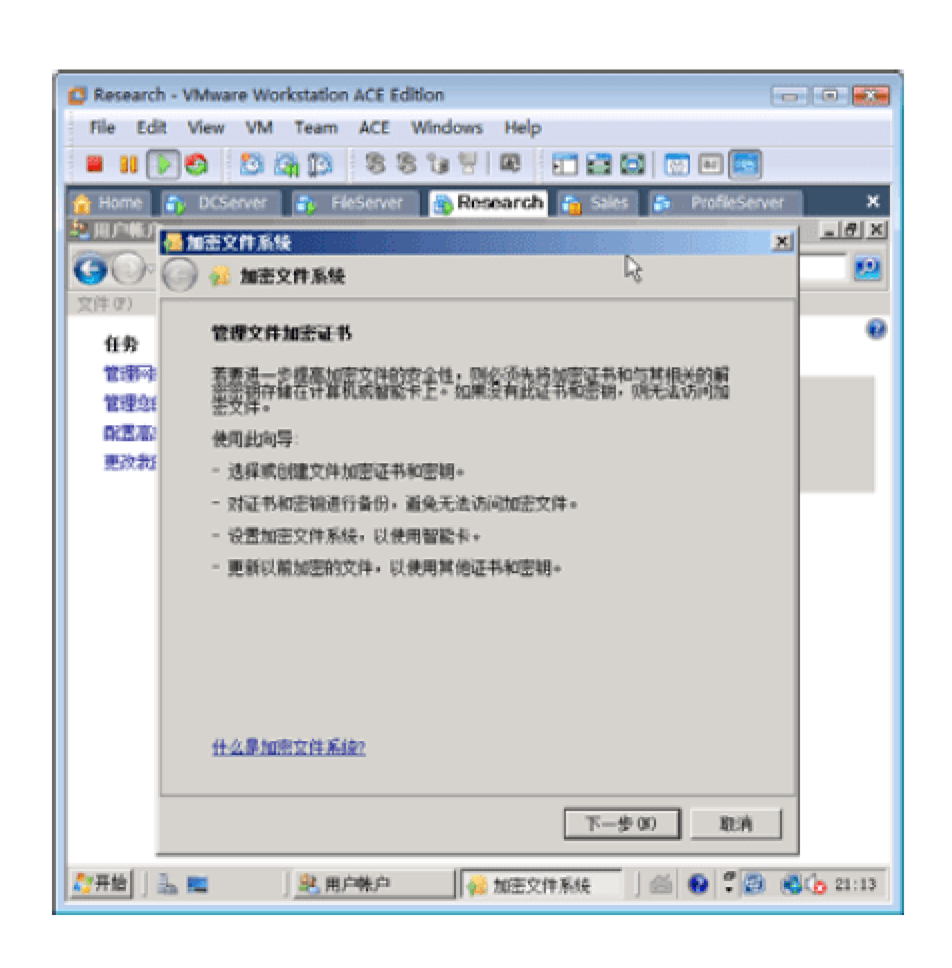


图 6-49　管理文件加密证书向导

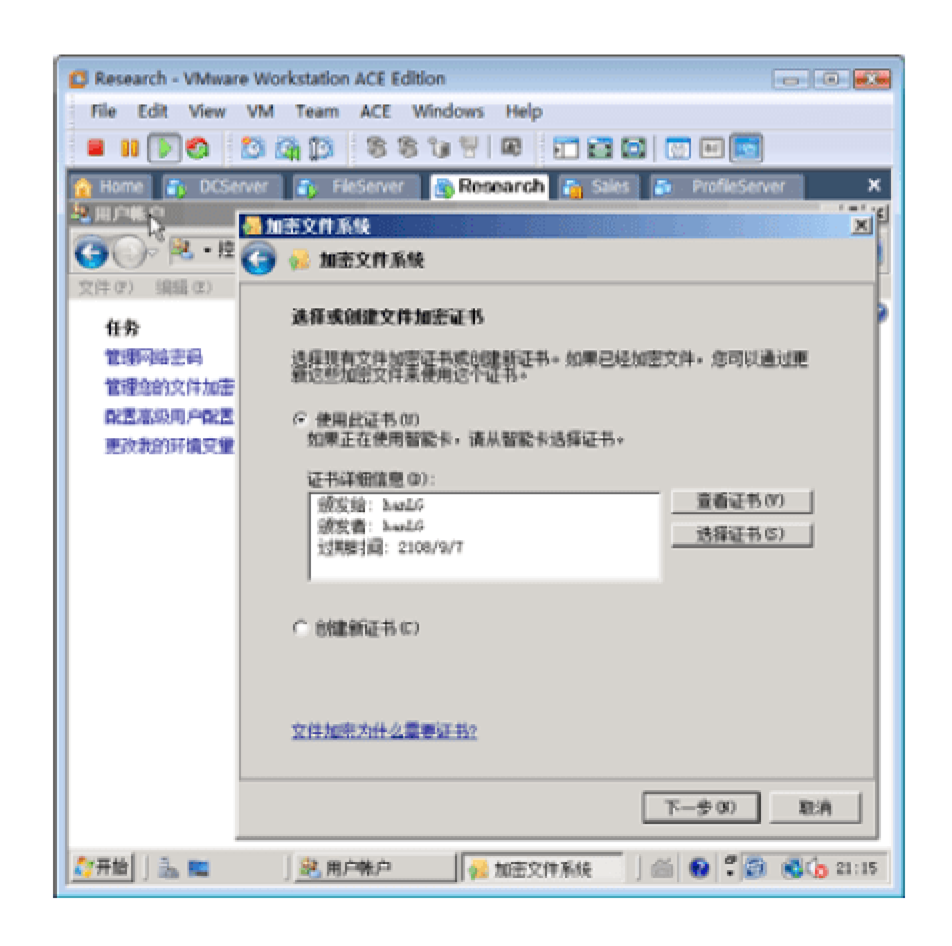


图 6-50　可以选择 EFS 使用的证书

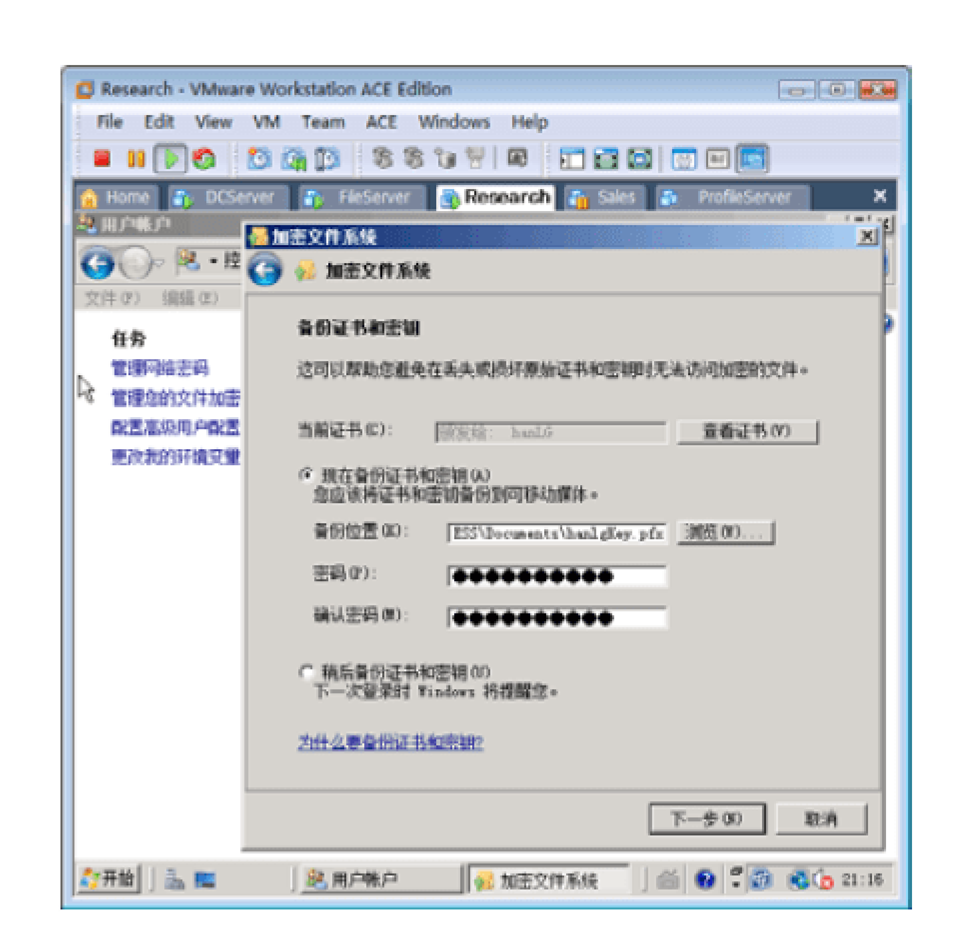


图 6-51　备份证书

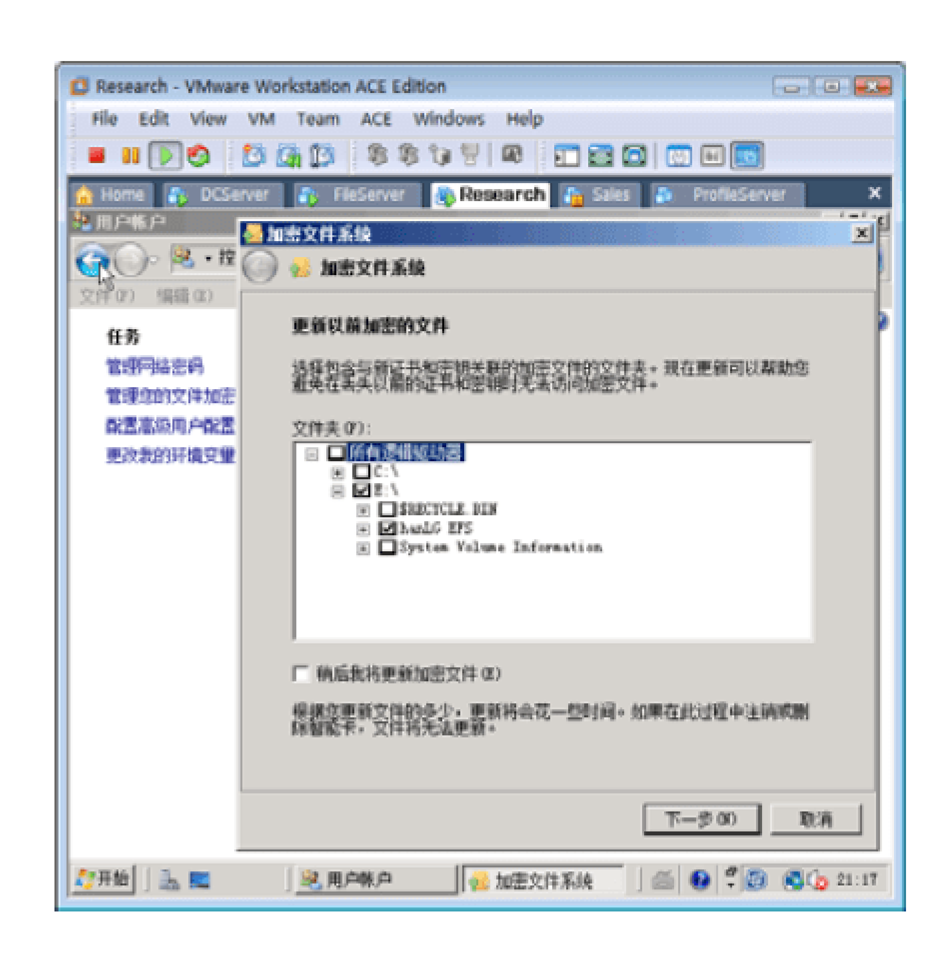


图 6-52　更新 EFS 加密的文件

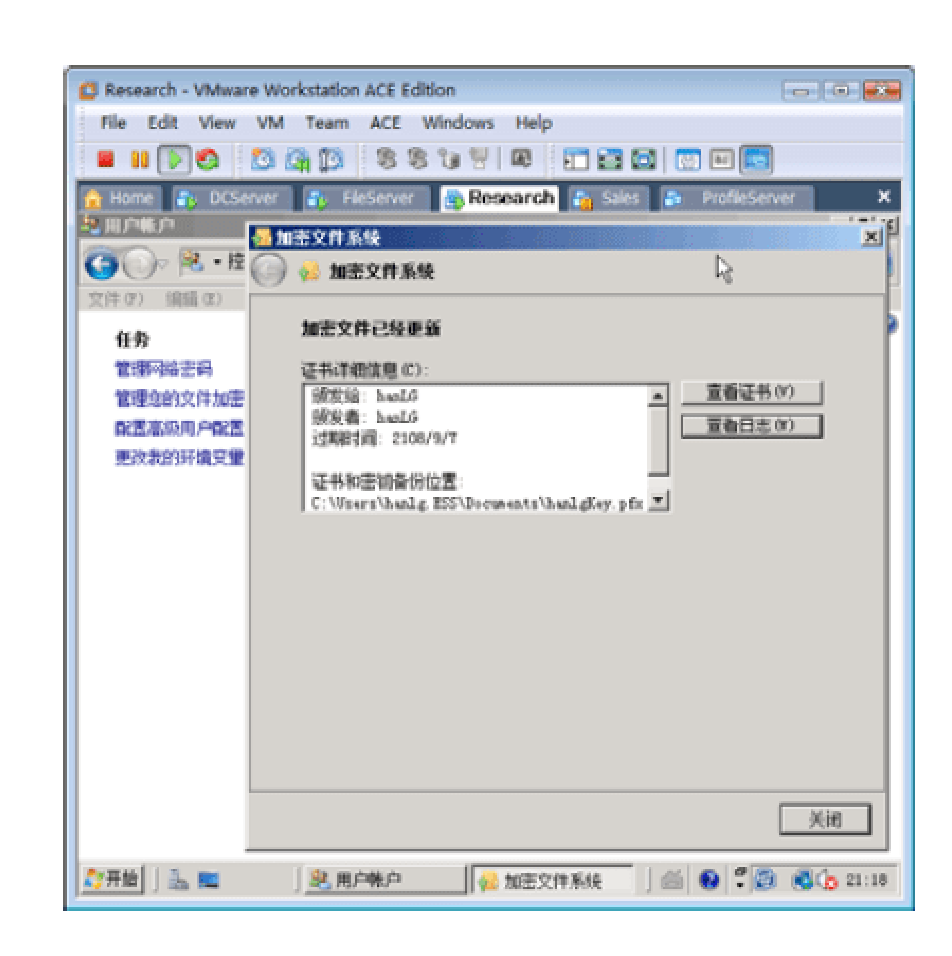


图 6-53　密钥备份成功



提示：这样所有的文件都使用现在的证书加密，避免现在备份的证书不能解密这些加密的文件夹。

3. 通过证书管理单元备份证书

① 选择“开始”→“运行”命令，在打开的“运行”对话框中输入 certmgr.msc，按 Enter 键。

② 如图 6-54 所示，在出现的证书窗口中双击展开“证书-当前用户”→“个人”→“证书”节点。

③ 此时，右侧窗格中会出现以你的用户名为名称的证书。选中该证书后右击，在弹出的快捷菜单中选择“所有任务”→“导出”命令，打开“证书导出向导”对话框。



提示：在向导进行过程中，当出现“是否要将私钥跟证书一起导出”提示时，应选择“是，导出私钥”选项，接着会出现向导提示要求密码的对话框。为了安全起见，可以设置证书的安全密码。

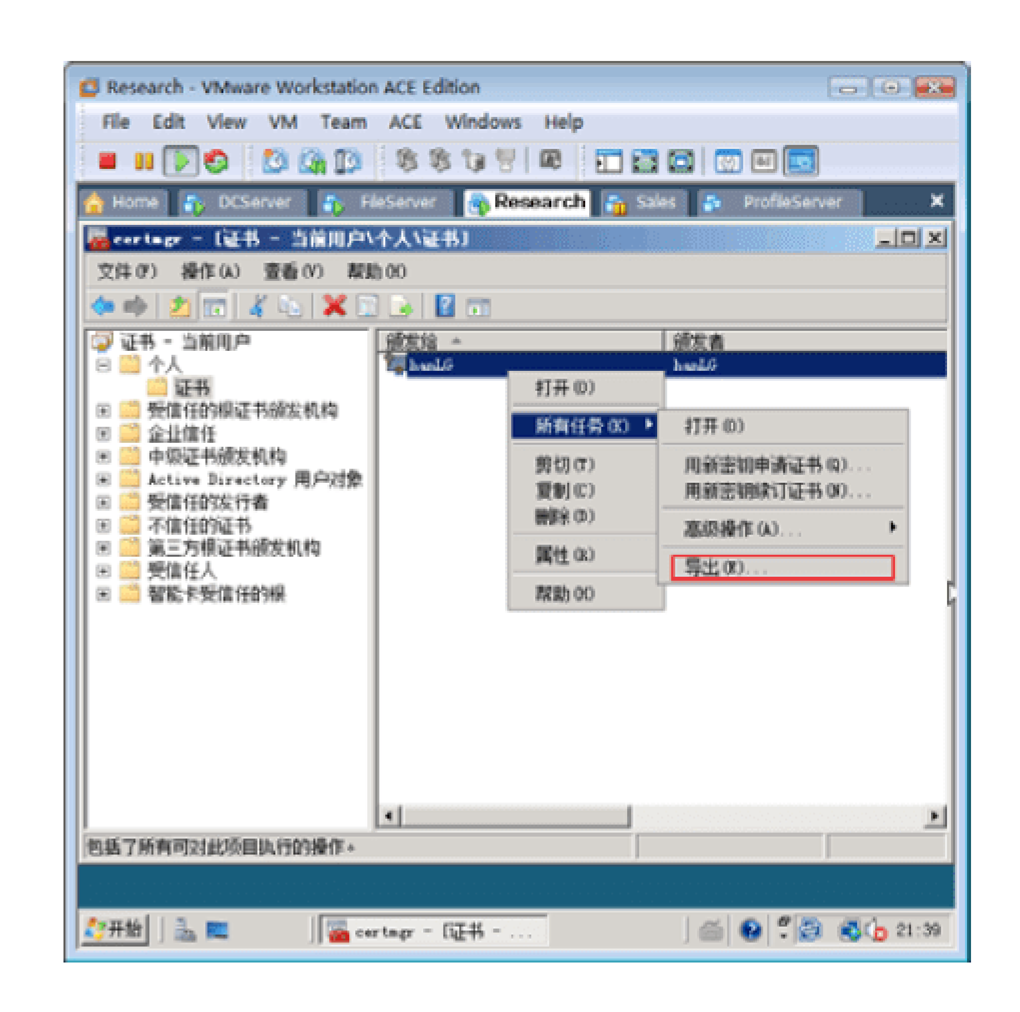


图 6-54　打开证书管理工具

④ 当选择好保存的文件名及文件路径后，单击“完成”按钮即可顺利将证书导出。此时会发现在保存路径上出现一个以 PFX 为扩展名的文件。



提示：当其他用户或重装系统后欲使用该加密文件时，只需记住证书及密码，然后在该证书上右击，在弹出的快捷菜单中选择“安装证书”命令，即可进入“证书导入向导”对话框。按默认状态单击“下一步”按钮，输入正确的密码后，即可完成证书的导入，这样即可顺利打开所加密的文件。

6.4.3　导入其他用户的 EFS 证书

导入其他用户的 EFS 证书，可以打开其加密的文件。

示例：域账户韩旭导入韩立刚账户备份的 EFS 证书打开其加密的文件。

① 韩立刚账户将其导出的 EFS 证书备份到“公用”文件夹中“公用图片”中。

> **提示：**韩旭用户账户没有权限访问韩立刚账户的“我的文档”，将 EFS 证书放到“公用”文件夹中的“公用图片”文件夹的目的是为了韩旭能够访问韩立刚的 EFS 证书。

② 以域账户“韩旭”登录到 Research 计算机。双击 hanLG EFS 文件夹中的 hanLG Test.txt，系统提示“拒绝访问”，如图 6-55 所示。

③ 如图 6-56 所示，打开 IE 属性对话框，切换到“内容”选项卡，单击“证书”按钮，在出现的“证书”对话框中，单击“导入”按钮。

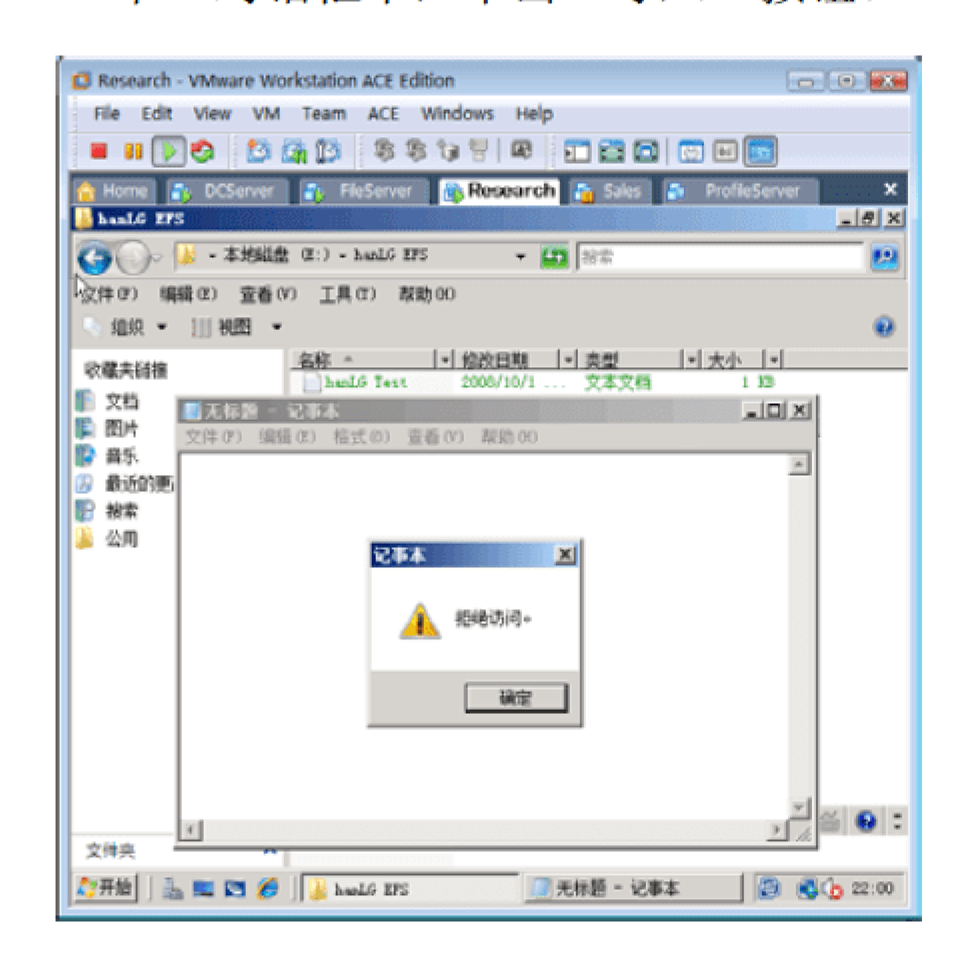



图 6-55　解密失败不能访问

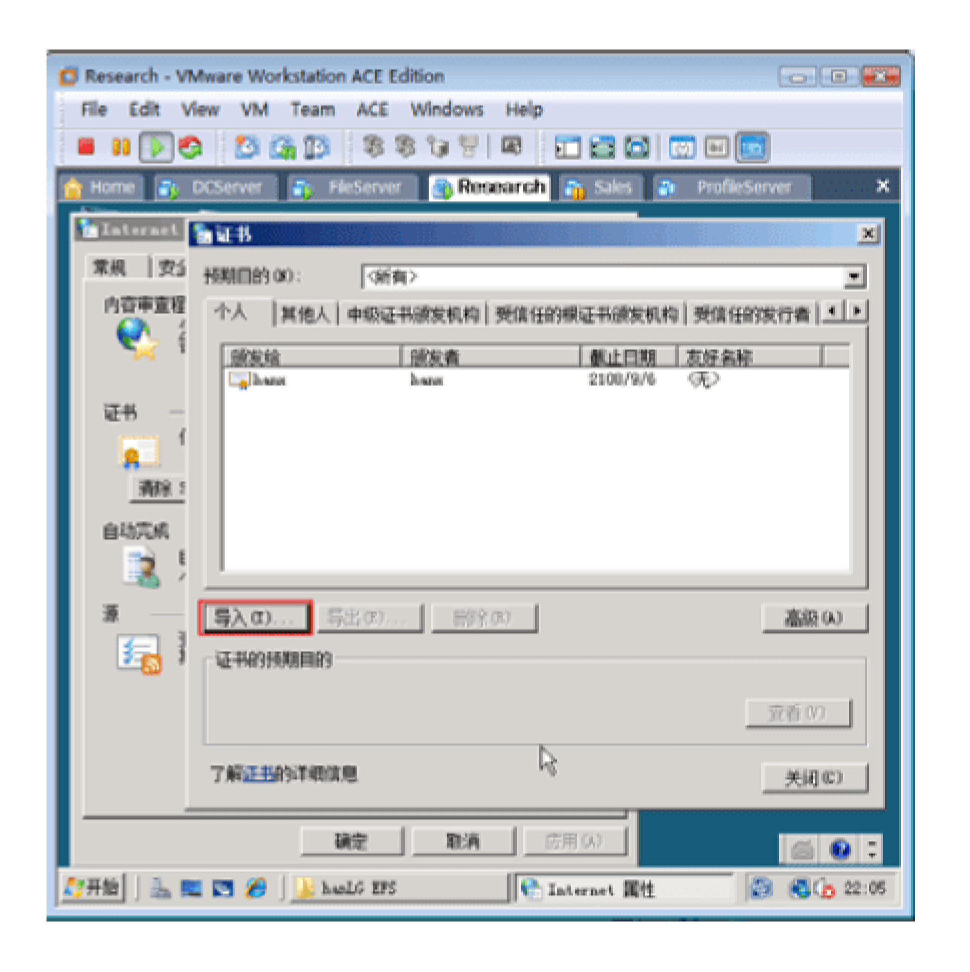


图 6-56　导入韩旭的 EFS 证书

④ 浏览到“公用”文件夹中的“公用图片”文件夹，如图 6-57 所示，文件扩展名选中“个人信息交换*.pfx;*.p12”，选中要导入的证书，单击“打开”按钮。

⑤ 如图 6-58 所示输入私钥保护密码，选中“标志此密钥为可导出的密钥”复选框，单击“下一步”按钮。

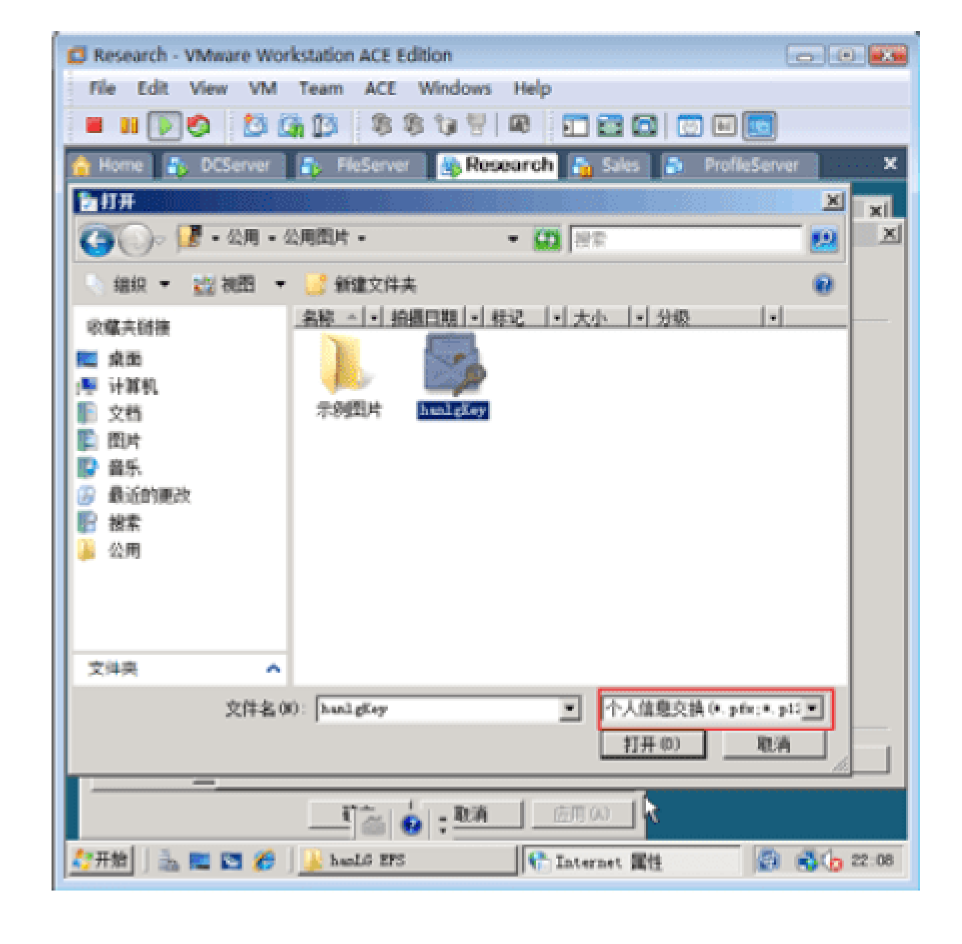


图 6-57　浏览到韩旭的 EFS 证书

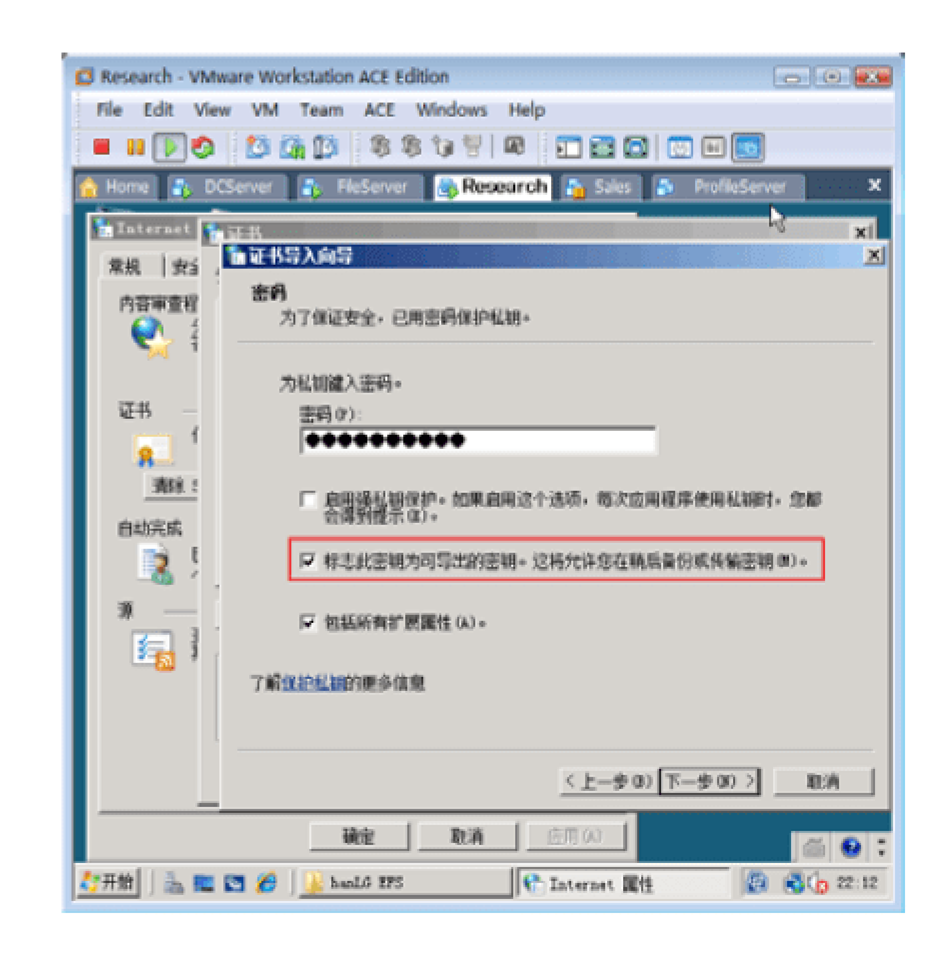


图 6-58　输入导入密钥

⑥ 如图 6-59 所示，在证书存储对话框中，默认为“个人”，单击“下一步”按钮，完成证书导入。你将看到两个可用的证书。

⑦　如图 6-60 所示，再次双击韩立刚加密的记事本文件，发现能够打开，说明解密成功。

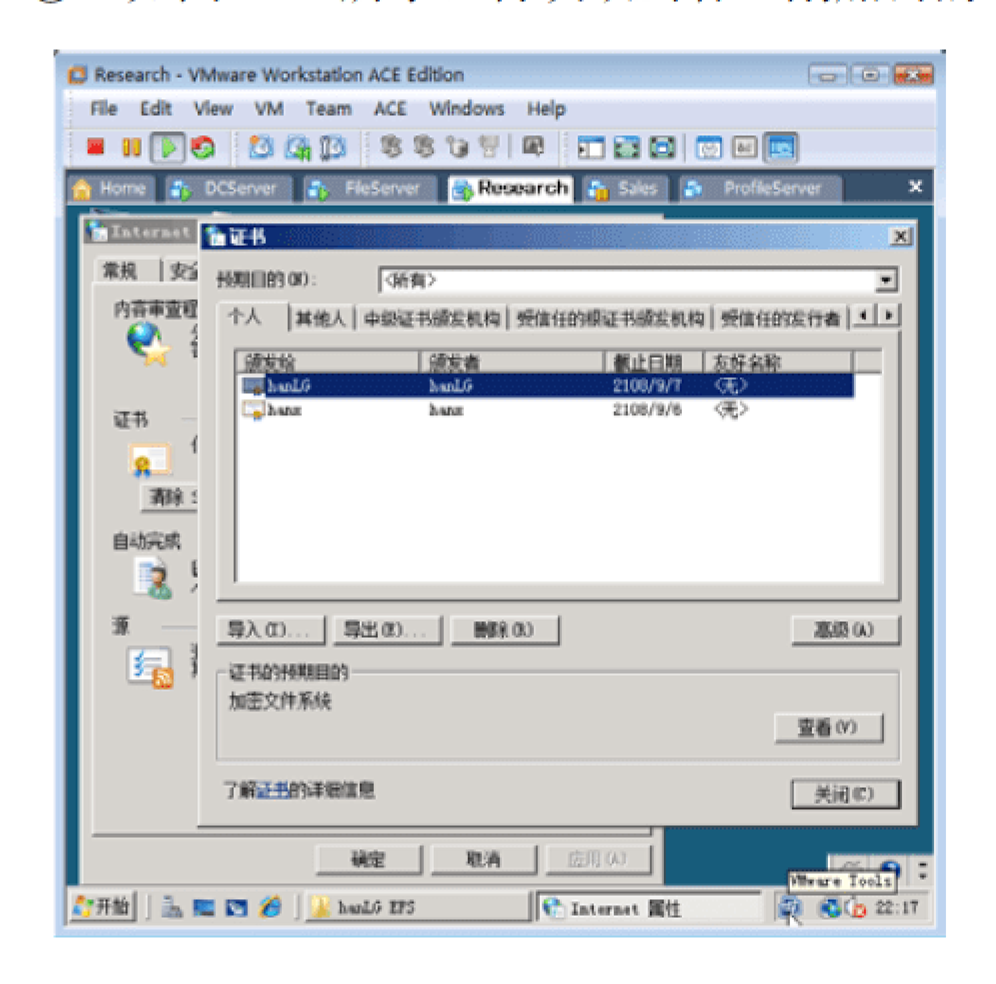


图 6-59　两个数字证书

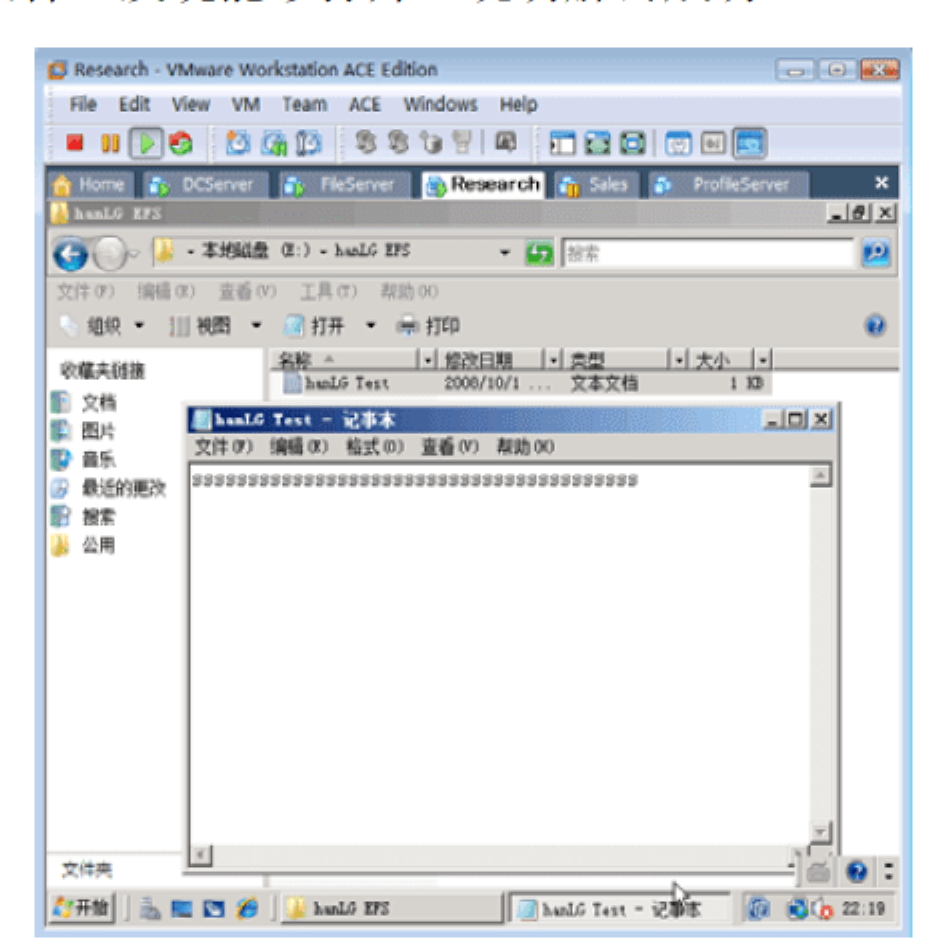


图 6-60　能够解密

6.4.4　共享 EFS 文件

你可能需要授权其他用户账户能访问你加密的文件，与使用同一个计算机的其他用户共享加密文件。

示例： 与使用同一个计算机的其他用户共享加密文件。

域用户账户“韩立刚”在 Research 计算机上加密的文件允许域用户“兰帅”账户访问。

①　以“兰帅”的域用户账户登录 Research 计算机，创建一个文件夹，并将其属性设置为加密。目的是让系统给“兰帅”分配一个 EFS 证书。

②　注销“兰帅”用户账户。

③　以韩立刚账户登录 Research 计算机，右击文件夹“hanLG EFS”文件夹中的“hanLG test.txt”文件，在弹出的快捷菜单中选择“属性”命令。



提示： 不能允许其他用户账户访问整个加密的文件夹。只能针对一个文件授权其他用户访问 EFS。

④　如图 6-61 所示，在属性对话框中，单击“高级”按钮，在出现的“高级属性”对话框中，单击“详细信息”按钮。

⑤　如图 6-62 所示，在出现的“用户访问”对话框中，单击“添加”按钮。

⑥　在出现的对话框中，列出了存储在本地计算机的用户配置文件中有 EFS 证书的用户的 EFS 证书。选中“兰帅”的 EFS 证书，单击“确定”按钮，如图 6-63 所示。完成授权。



提示： 这样加密该文件的对称密钥被这两个用户的 EFS 证书中的公钥加密了，因此两个用户账户都能够使用自己的私钥解密加密的对称密钥，使用该对称密钥再解密该文件。

⑦　以“兰帅”账户登录 Research 计算机，能够打开该记事本文件，如图 6-64 所示。

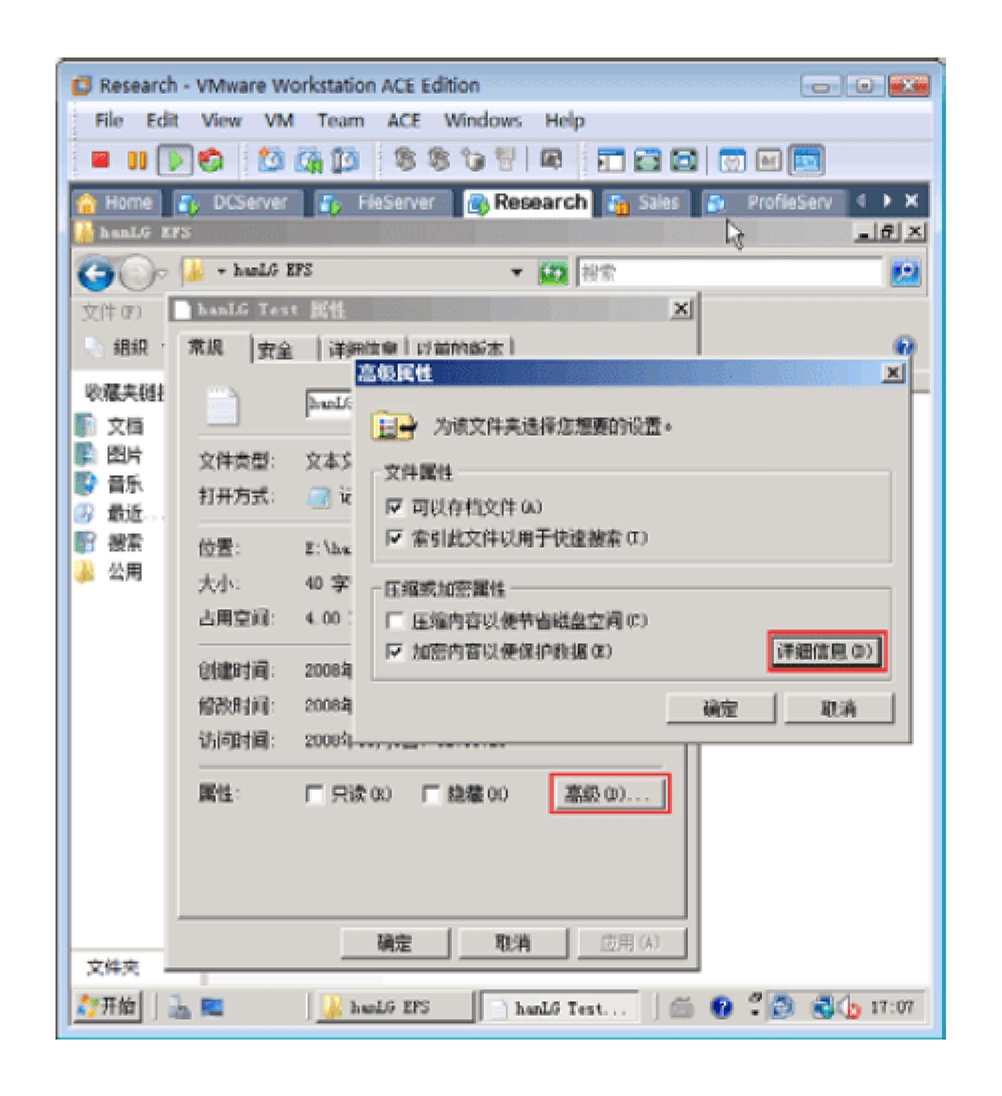


图 6-61 “高级属性”对话框

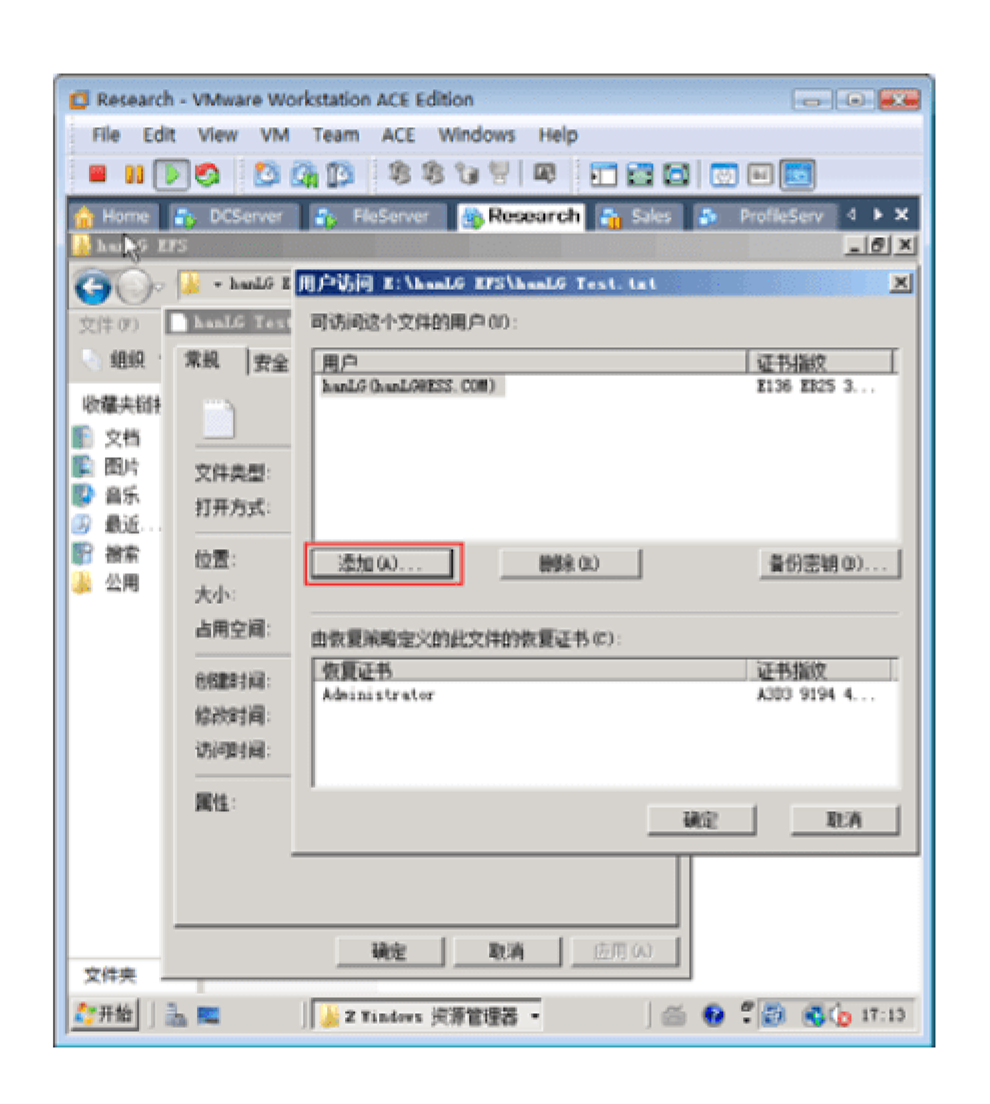


图 6-62 添加其他用户

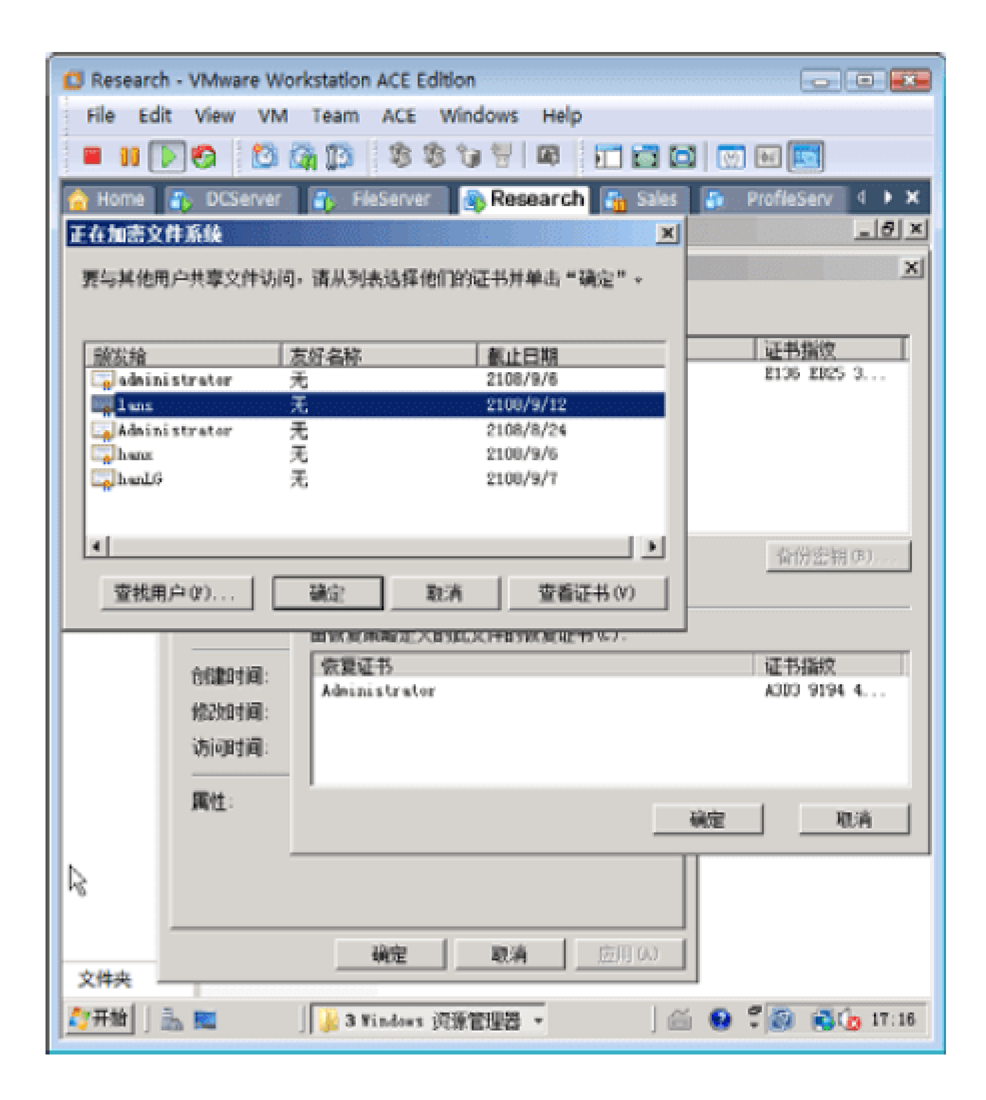


图 6-63 选择“兰帅”的 EFS 的数字证书

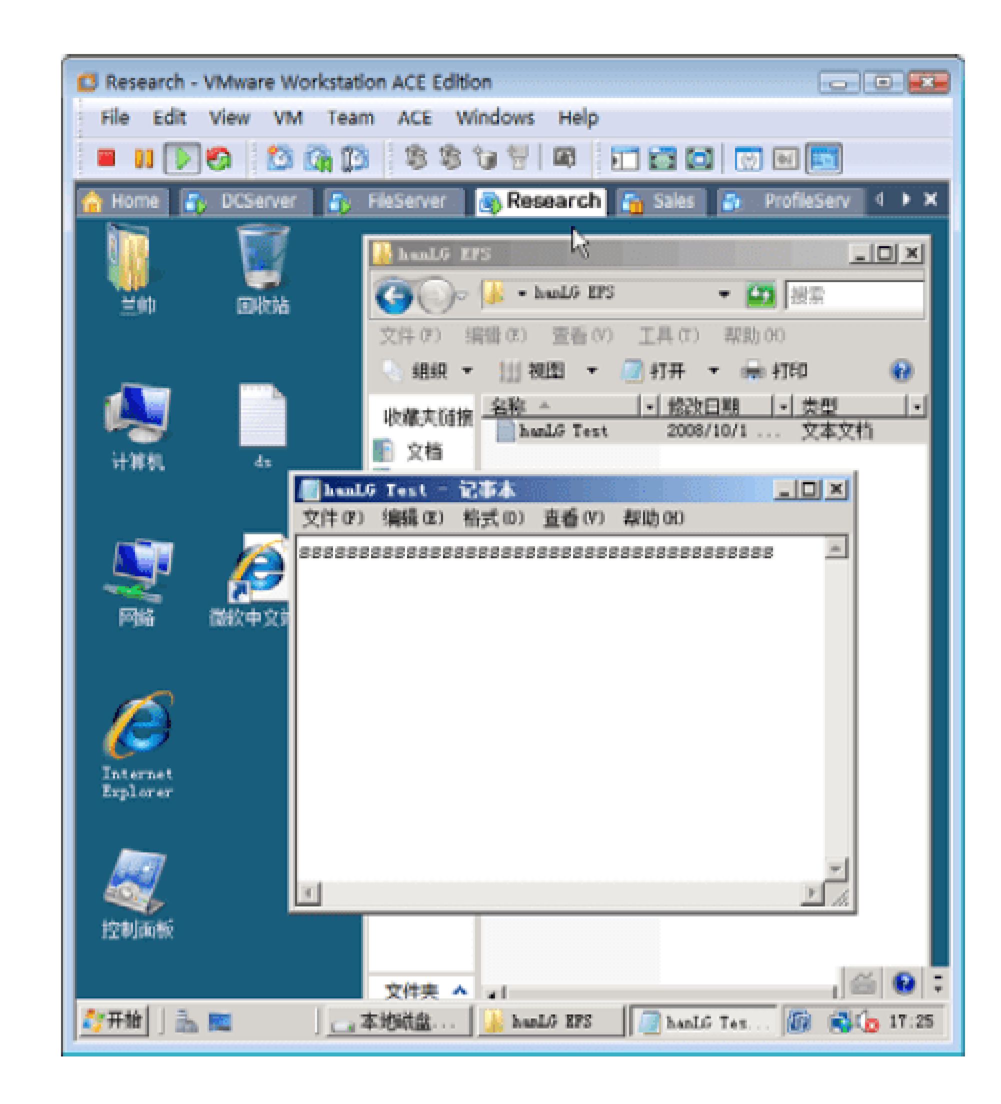


图 6-64 “兰帅”也能打开

6.4.5 在域环境中使用 EFS

在域环境中，可以安装活动目录证书服务，为域中的用户账户颁发 EFS 证书。这样使用漫游用户配置文件的用户账户，可以在域中的任何计算机访问自己加密的文件。

示例：在域环境中使用 EFS。

1. 任务

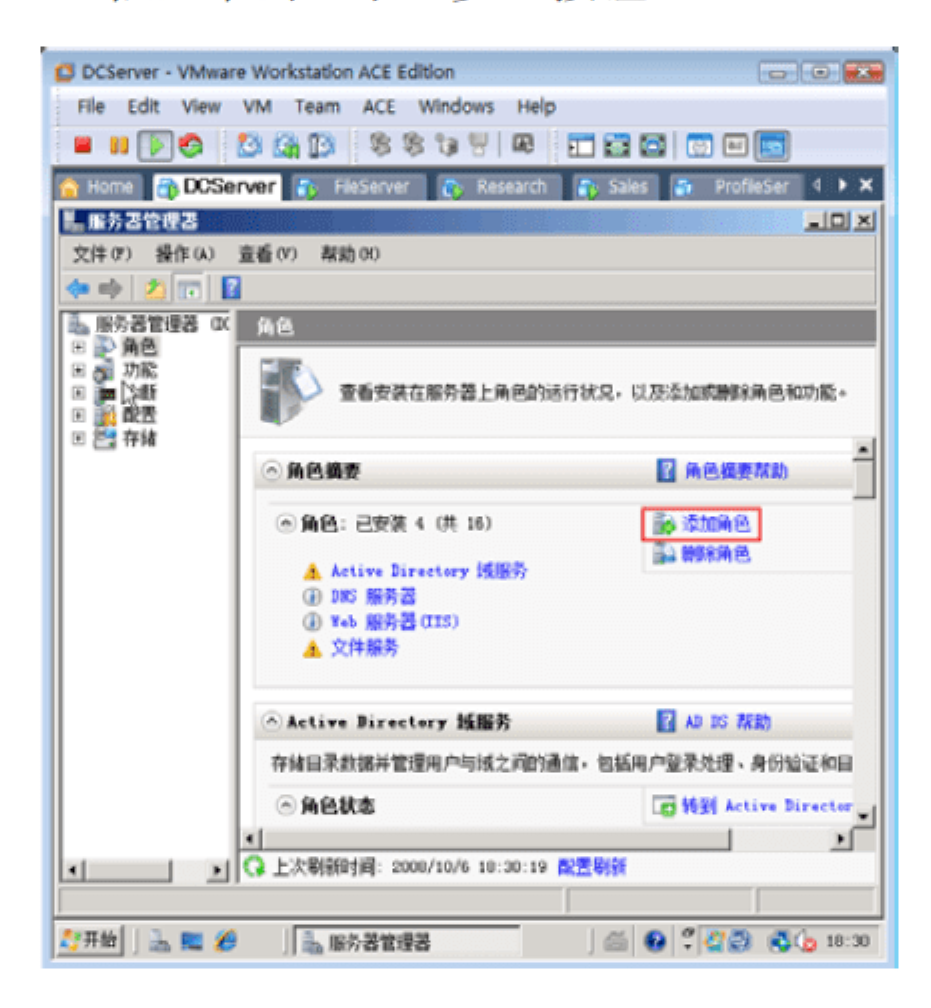
- 安装活动目录证书服务。
- 配置韩立刚用户账户使用漫游式配置文件。

- 使用新证书重新加密文件。
- 在 Research 计算机上共享 hanLG EFS 文件夹。
- “韩立刚”用户账户在 Sales 计算机登录访问 Research 计算机共享的 hanLG EFS 文件夹。
- 查看活动目录域用户的 EFS 证书。

2. 步骤

① 以域管理员的身份登录到 DCServer 上，如图 6-65 所示，打开“服务器管理器”窗口，单击“添加角色”按钮。

② 如图 6-66 所示，在出现的“选择服务器角色”界面中，选中“Active Directory 证书服务”复选框，单击“下一步”按钮。



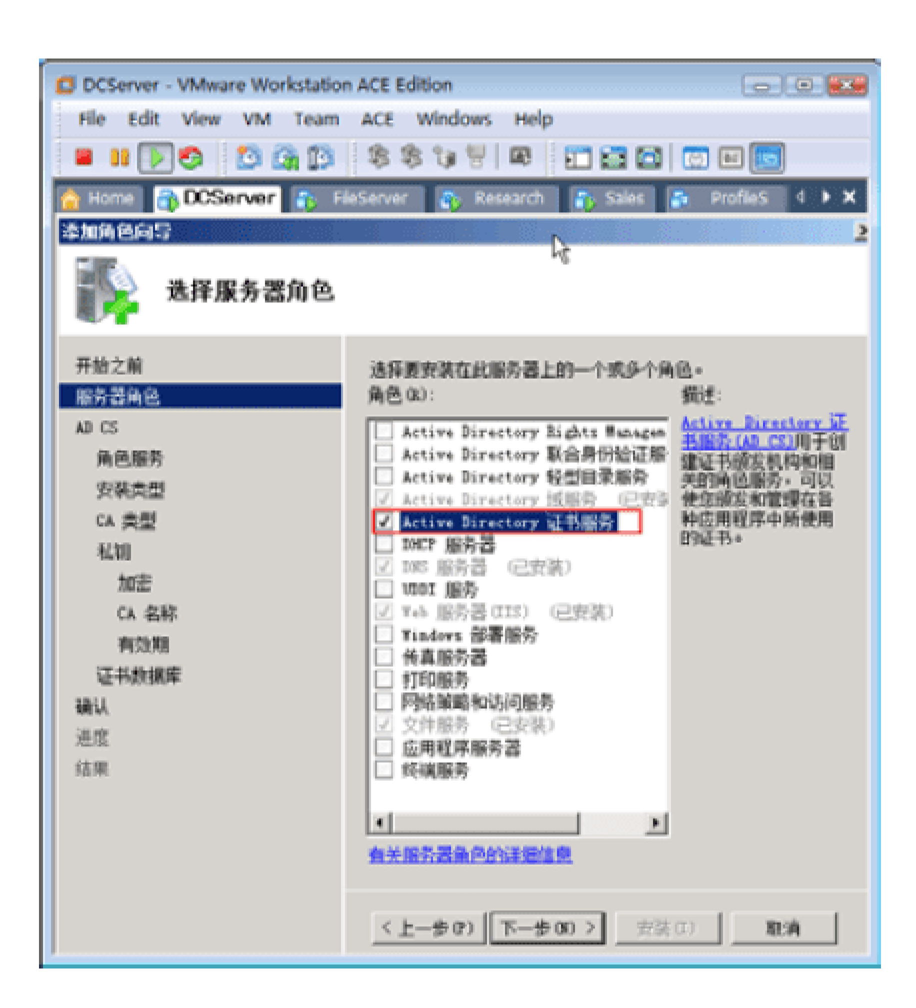
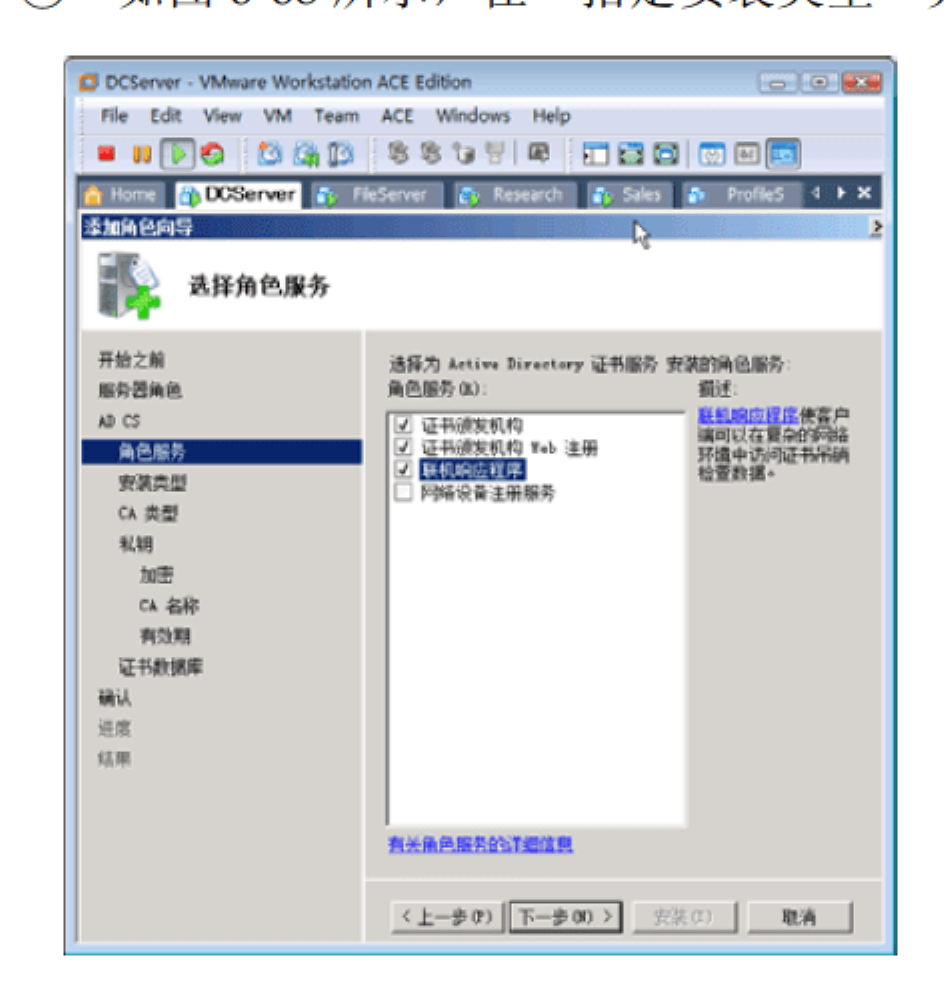



图 6-65　添加角色

图 6-66　选择活动目录证书服务

③ 如图 6-67 所示，在出现的“选择角色服务”界面中，选中“证书颁发机构”、“证书颁发机构 Web 注册”和“联机响应程序”复选框，单击“下一步”按钮。

④ 如图 6-68 所示，在“指定安装类型”界面中，选中“企业”单选按钮，单击“下一步”按钮。



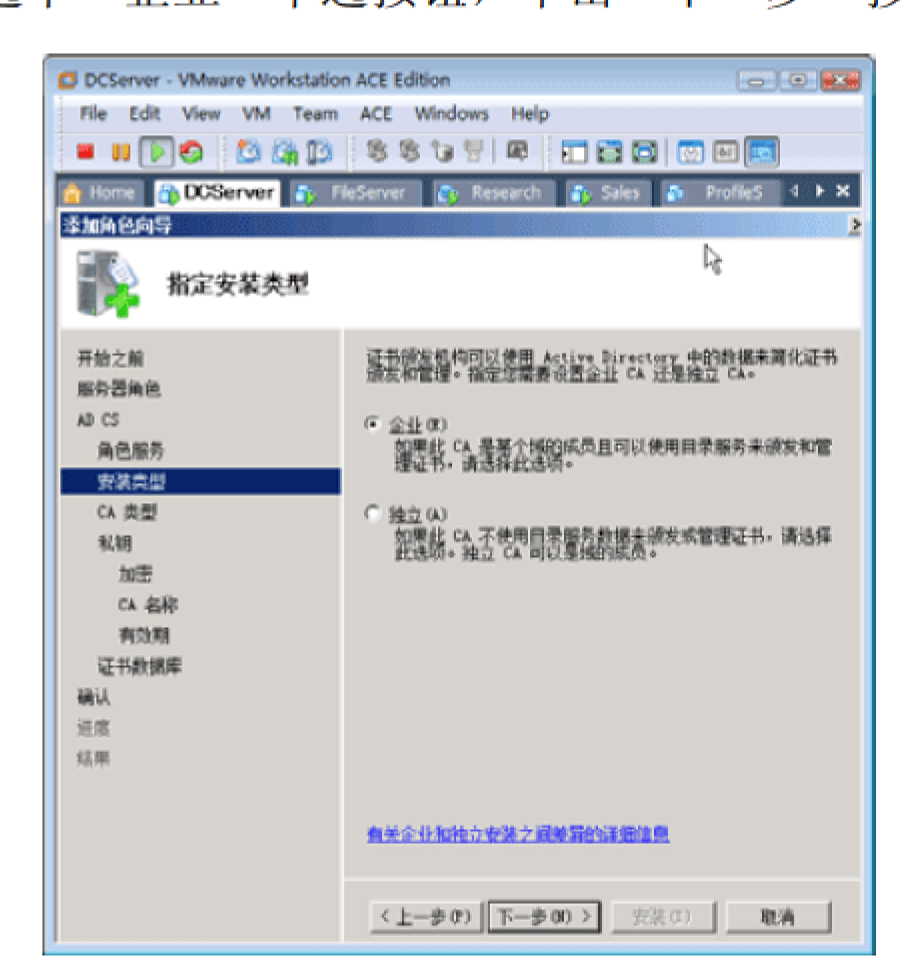


图 6-67　选择角色服务

图 6-68　指定安装类型

⑤ 如图 6-69 所示，在出现的“指定 CA 类型”界面中，选中“根 CA”单选按钮，单击“下一步”按钮。

⑥ 如图 6-70 所示，在出现的“设置私钥”界面中，选中“新建私钥”单选按钮，单击“下一步”按钮。

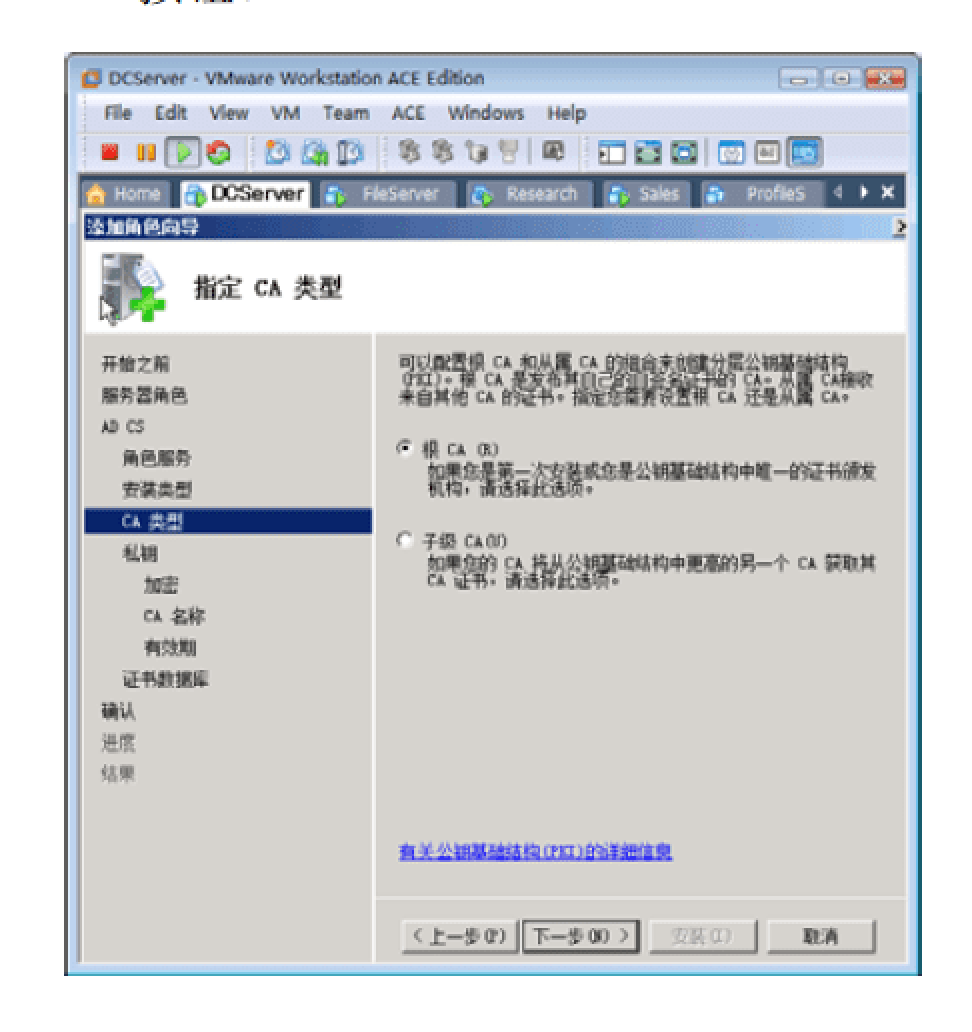


图 6-69 指定 CA 类型

图 6-70 设置私钥

⑦ 如图 6-71 所示，在“为 CA 配置加密”界面中，密钥长度选中 2048，单击“下一步”按钮。

⑧ 如图 6-72 所示，在出现的“配置 CA 名称”界面中，输入此 CA 公用名称，单击“下一步”按钮。

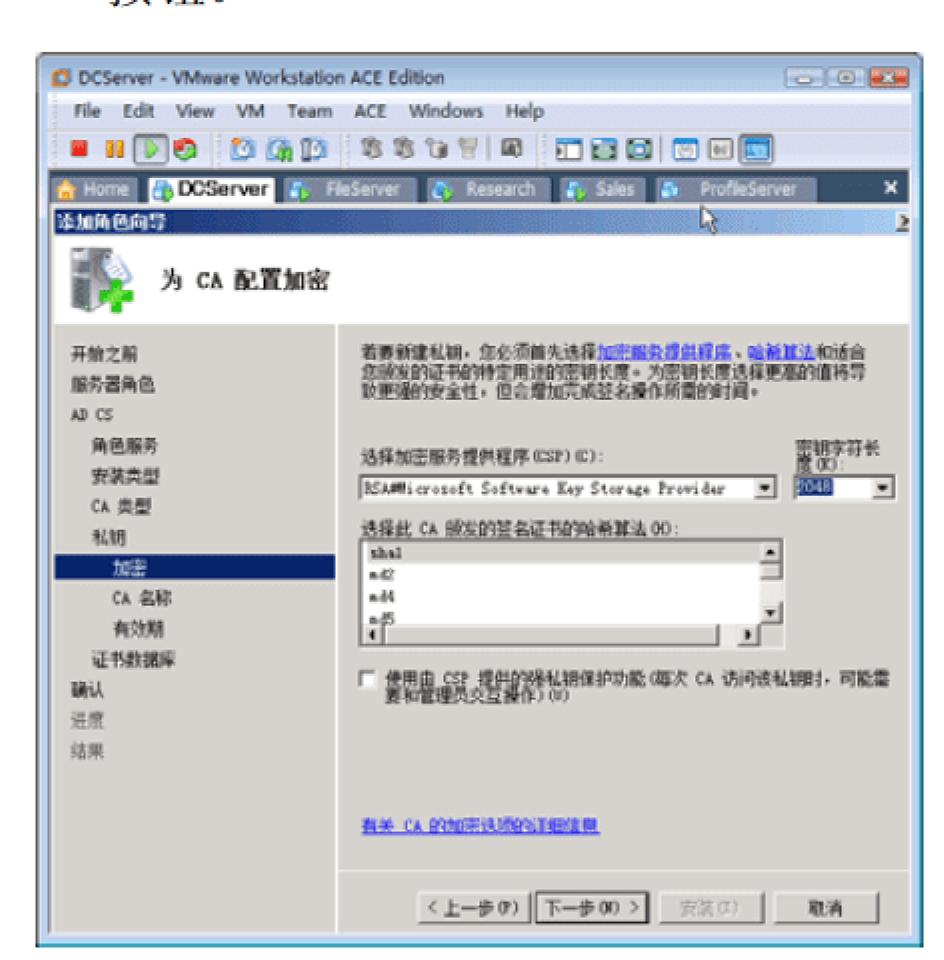


图 6-71 为 CA 配置加密

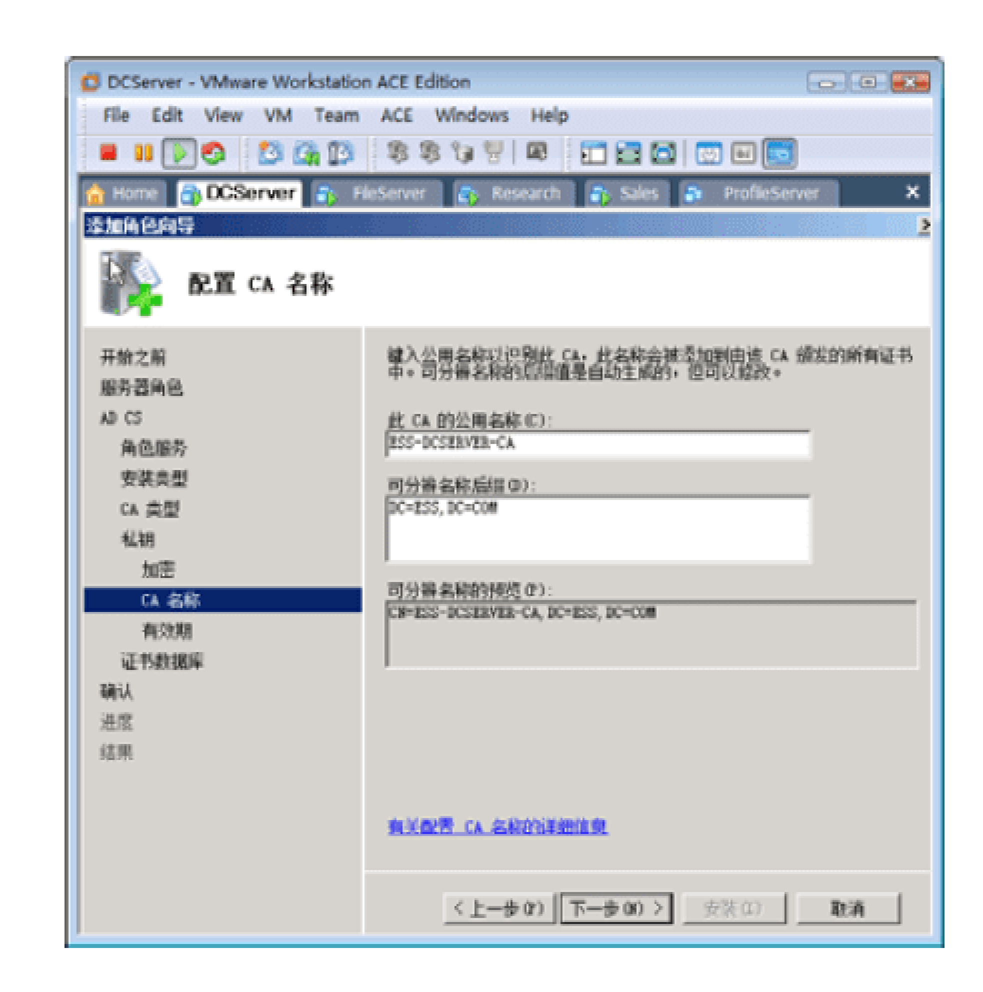


图 6-72 配置 CA 名称

⑨ 如图 6-73 所示，在出现的“设置有效期”界面中，指定证书的有效期，单击“下一步”按钮。

⑩ 如图 6-74 所示，在出现的“配置证书数据库”对话框中，选择证书数据库和日志的位置，单击“下一步”按钮，完成安装过程。

⑪ 如图 6-75 所示，将韩立刚的用户账户配置文件指定到 FileServer 上的 profiles 文件夹中。

注意：使用用户漫游式配置文件，使得用户的 EFS 证书在域中的任何计算机都可用。

⑫ 在 Research 计算机和 Sales 计算机上运行 gpupdate /force 命令来强制计算机刷新策略，这样他们就能自动发现域中安装的证书颁发机构了，并且信任该证书颁发机构。

⑬ 以韩立刚用户账户登录到 Research 计算机，选择“开始”→“设置”→“控制面板”→“用户账户”命令。

⑭ 打开如图 6-76 所示的“用户帐户”窗口，单击“管理您的文件加密证书”选项。

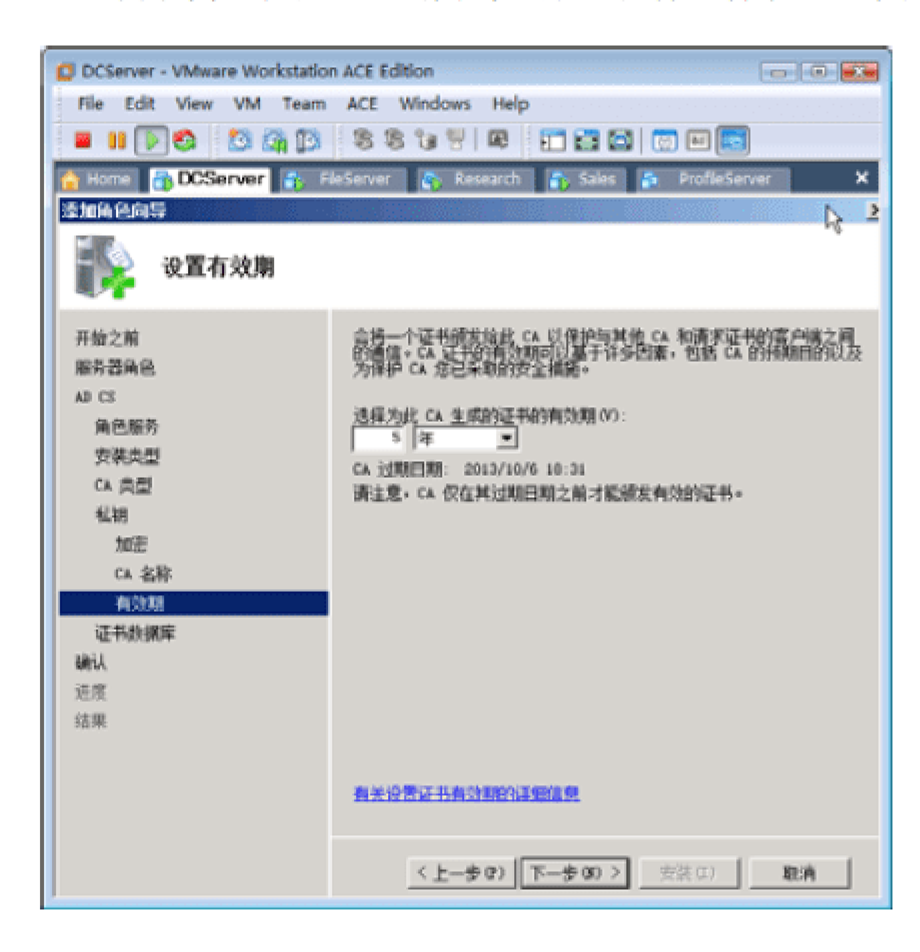


图 6-73　设置有效期

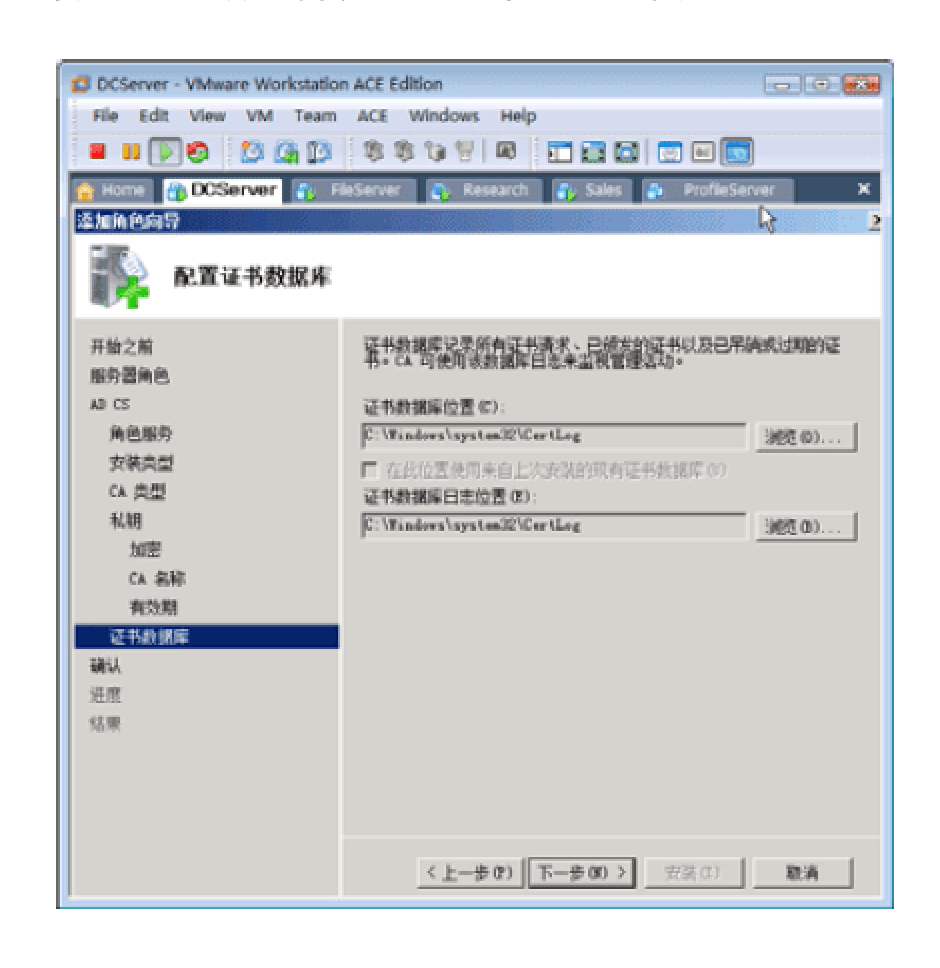


图 6-74　配置数据库

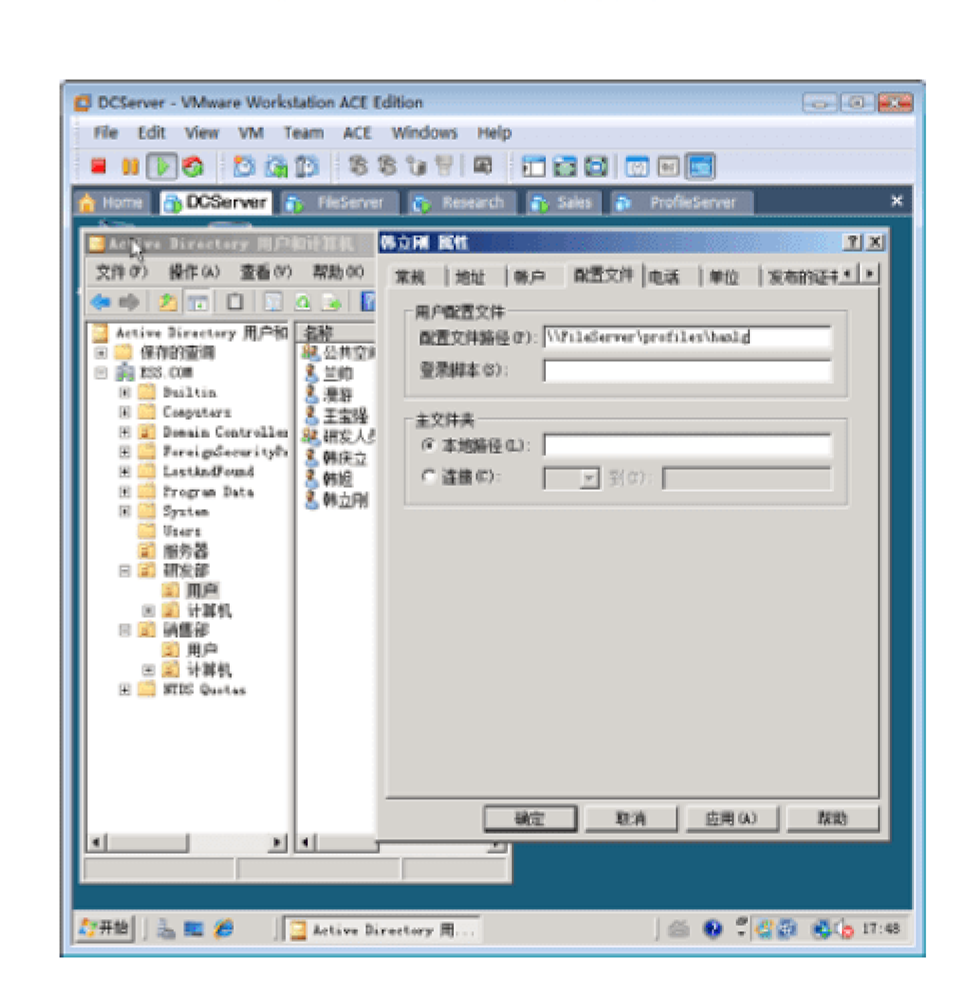


图 6-75　指定漫游式配置文件

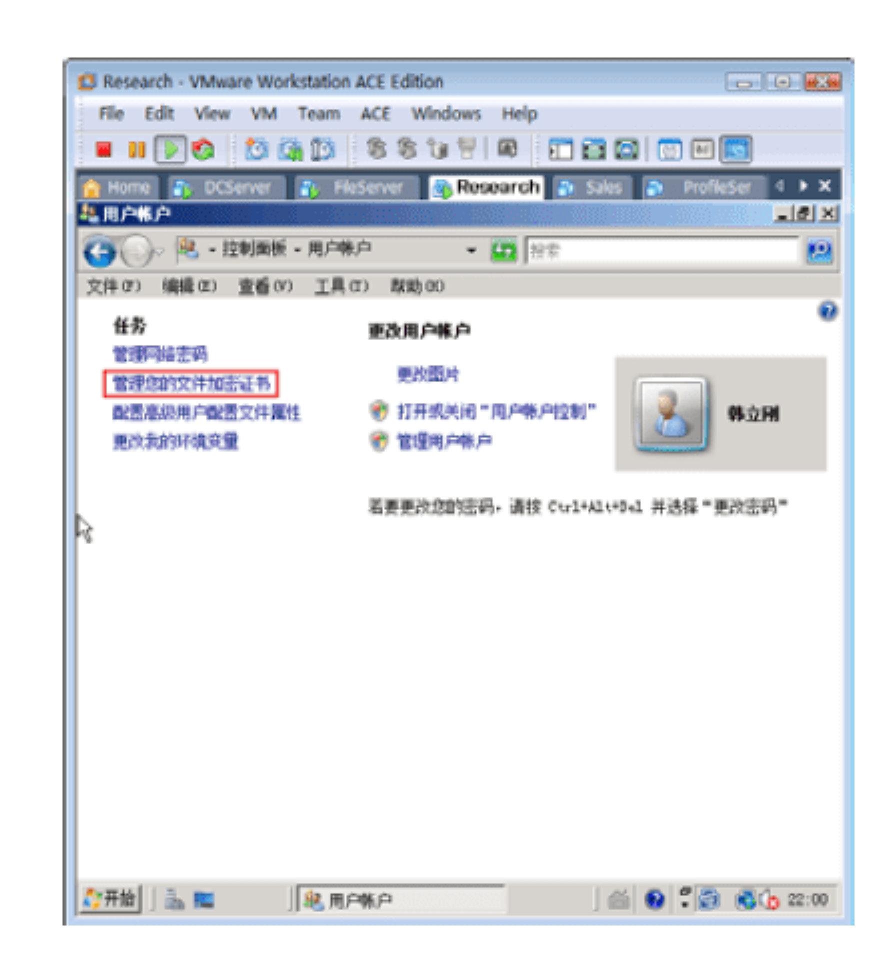


图 6-76　管理文件加密证书

⑮ 如图 6-77 所示，在“选择或创建文件加密证书”界面中，选中“创建新证书”单选按钮，单击“下一步”按钮。

⑯ 如图 6-78 所示，在出现的选择证书类型对话框中，选中“域证书颁发机构颁发的证书”单选按钮，单击“下一步”按钮。

⑰ 如图 6-79 所示，在出现的“备份证书和密钥”界面中，单击“稍后备份证书和密钥”单选按钮，单击“下一步”按钮。

⑱ 如图 6-80 所示，在“更新以前加密的文件”界面中，选中 hanLG EFS 文件夹，单击“下一步”按钮。

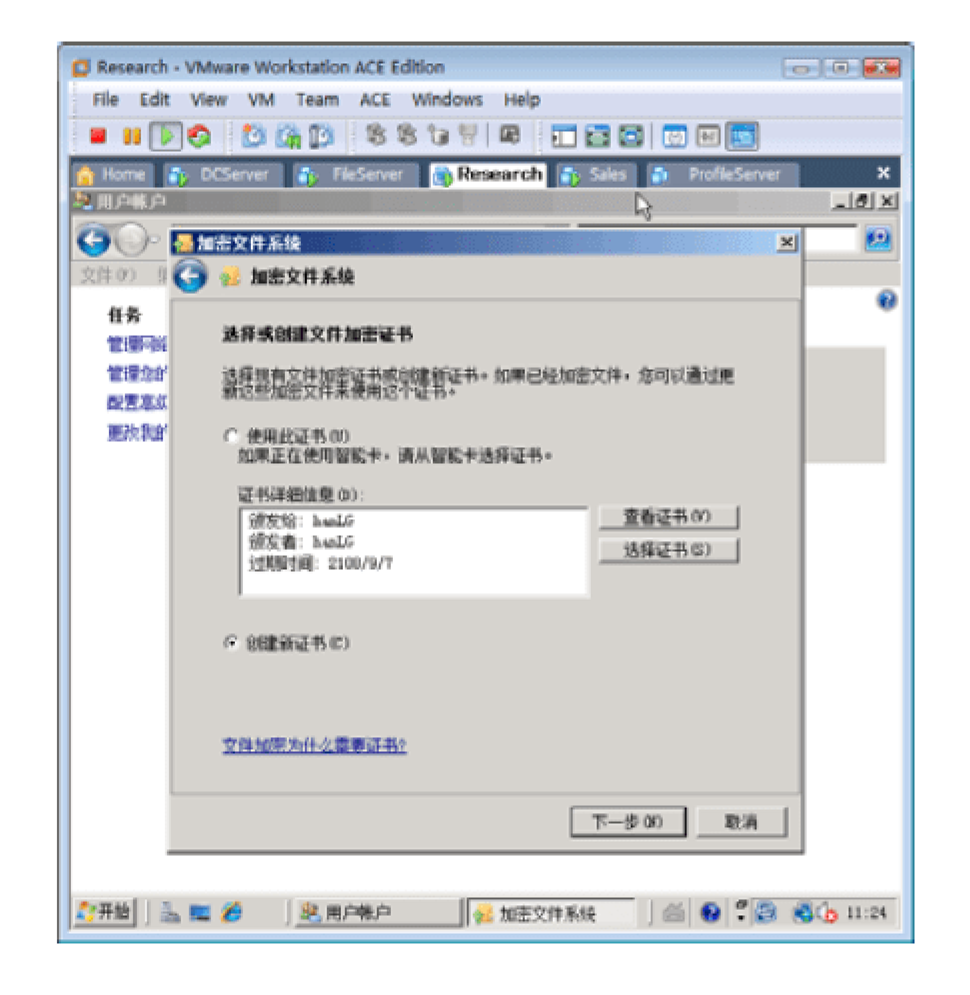


图 6-77 创建证书

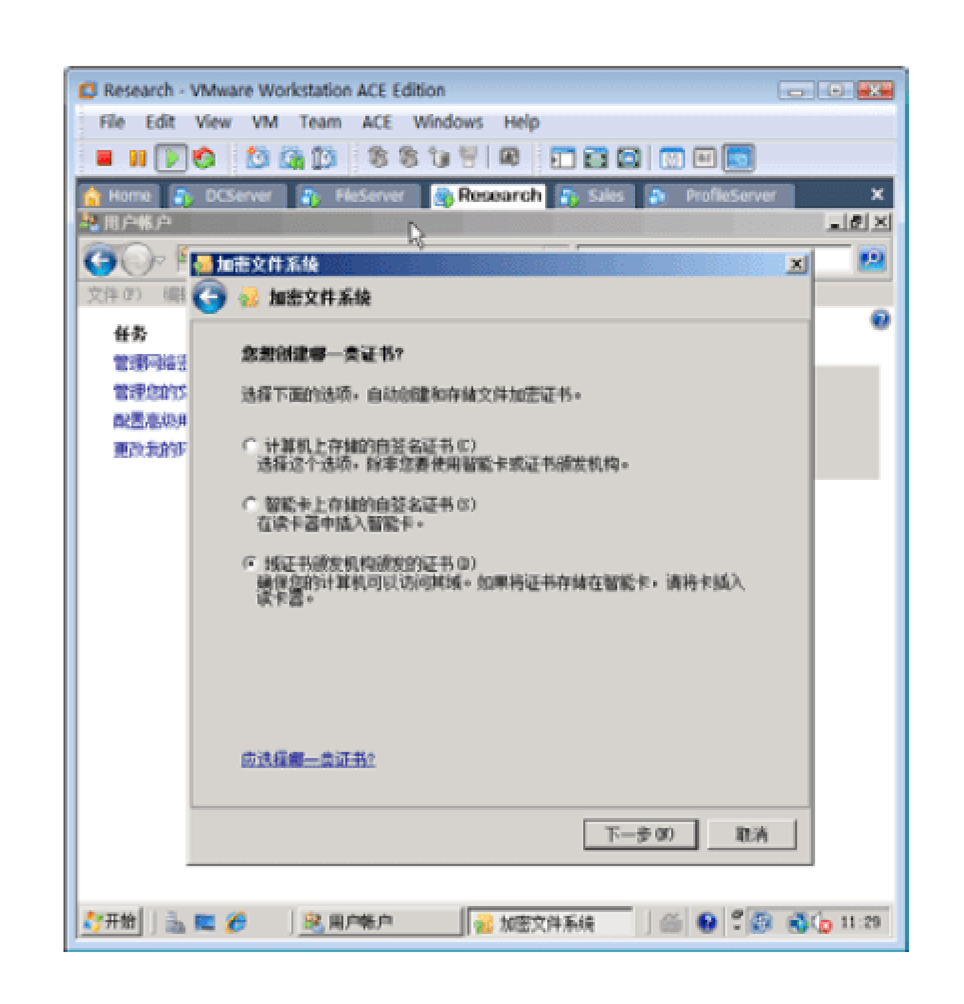


图 6-78 选择证书类型



提示：通过更新以前加密的文件夹，该文件夹中的文件将会使用新的 EFS 证书加密。

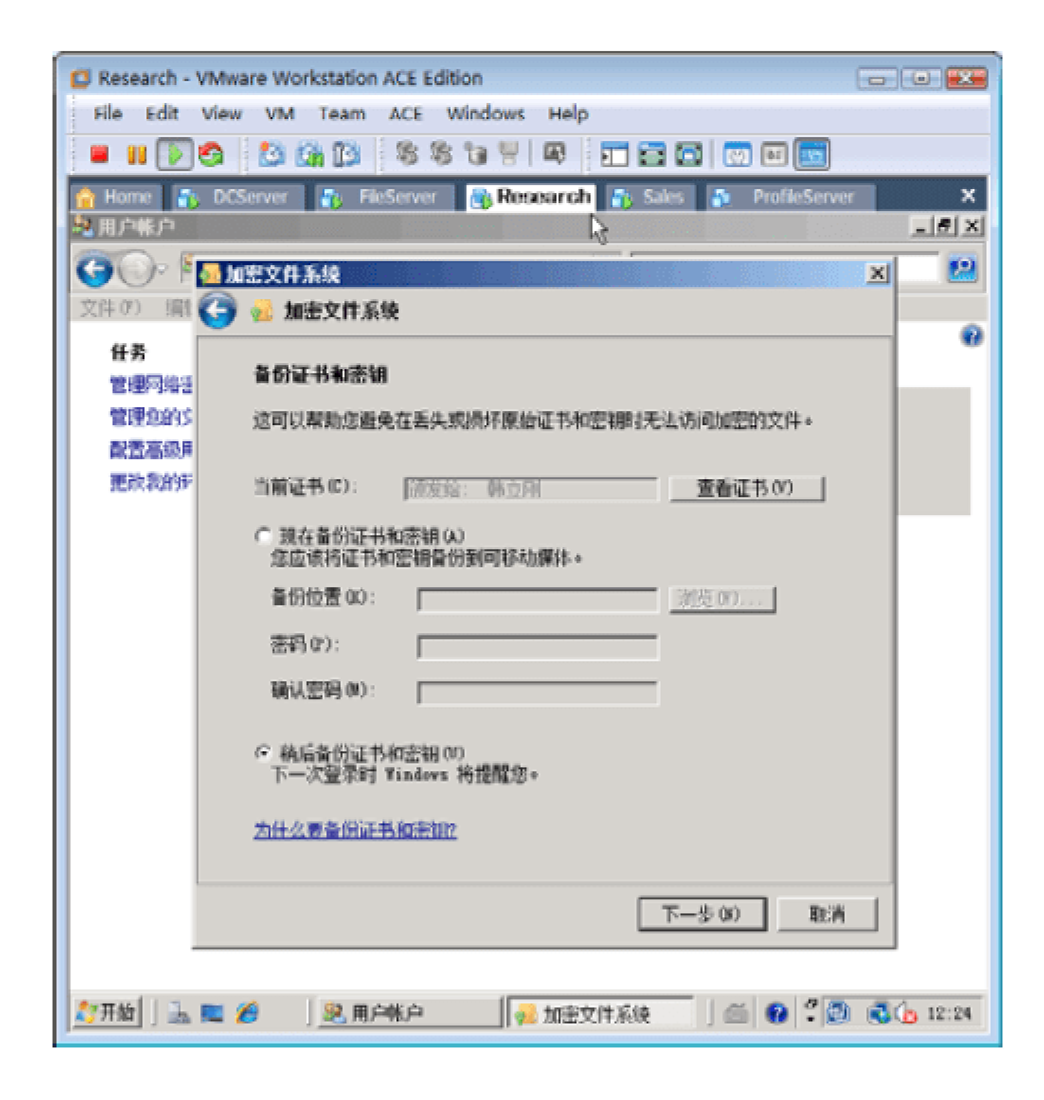


图 6-79 备份证书和密钥

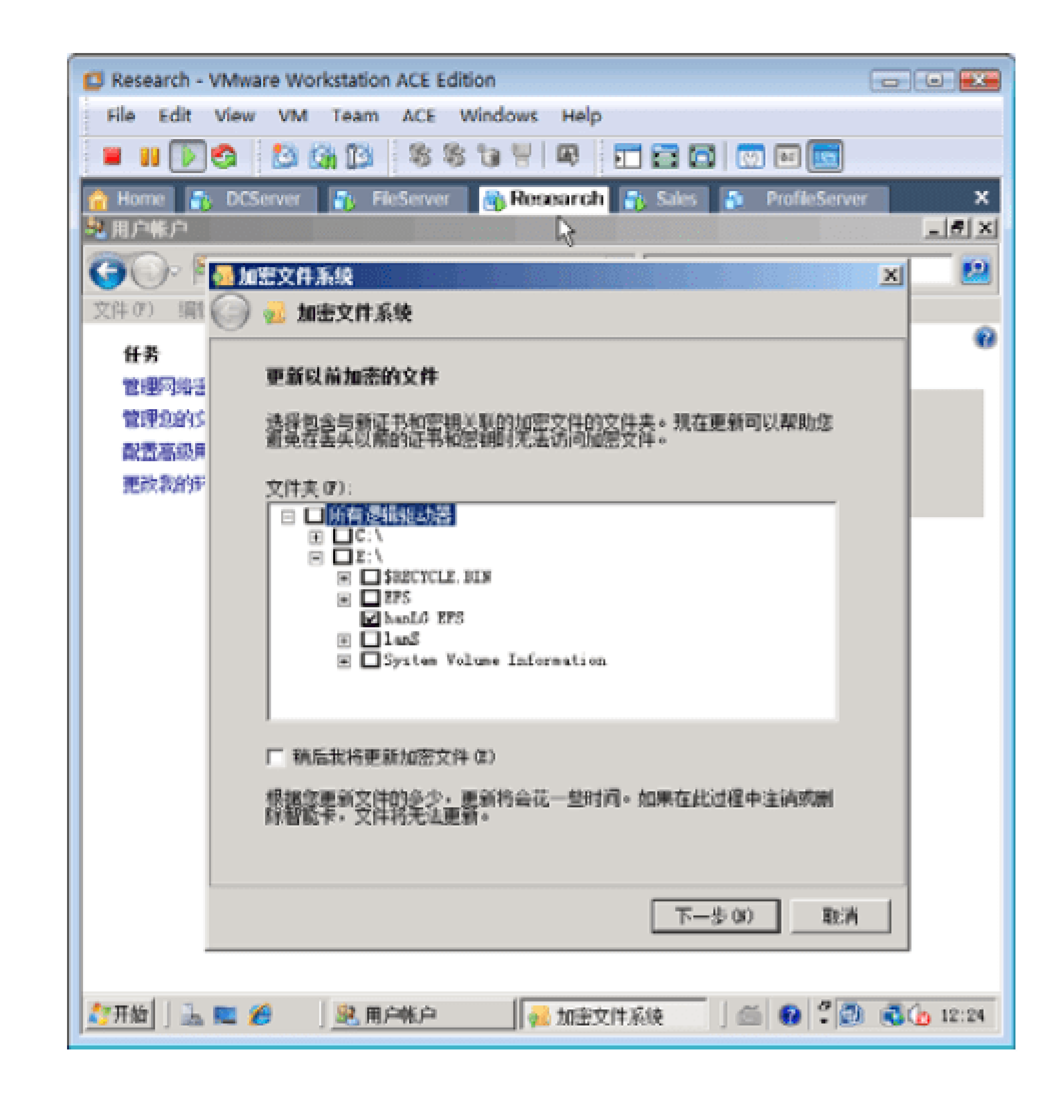


图 6-80 更新以前加密的文件

⑲ 如图 6-81 所示，在出现的“某些加密的文件没有更新”界面中，单击“查看证书”按钮。

⑳ 如图 6-82 所示，在“证书”对话框的“常规”选项卡中，可以看到颁发者是 ESS-DCSERVER-CA。依次单击“确定”和“关闭”按钮。



注意：此时，可以看到你有一个与该证书对应的私钥。

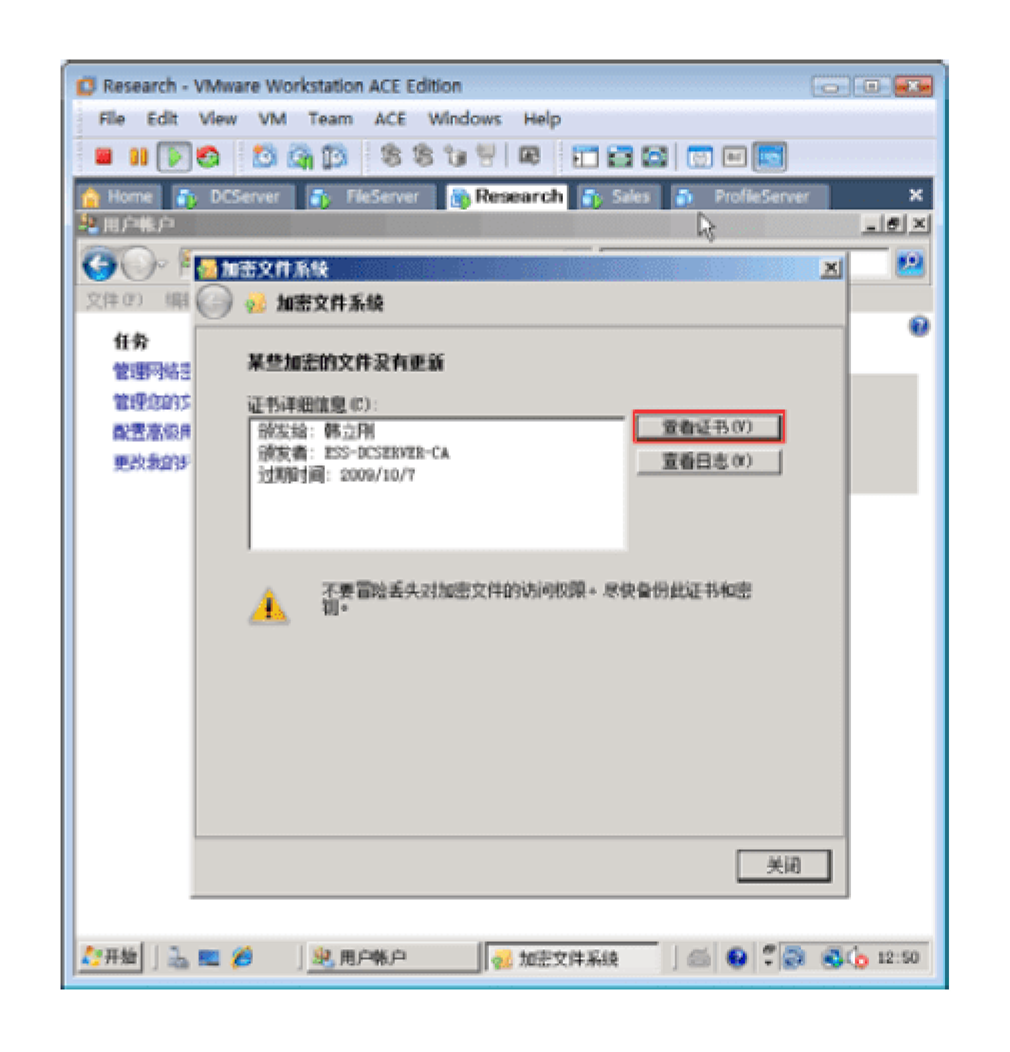


图 6-81　查看证书

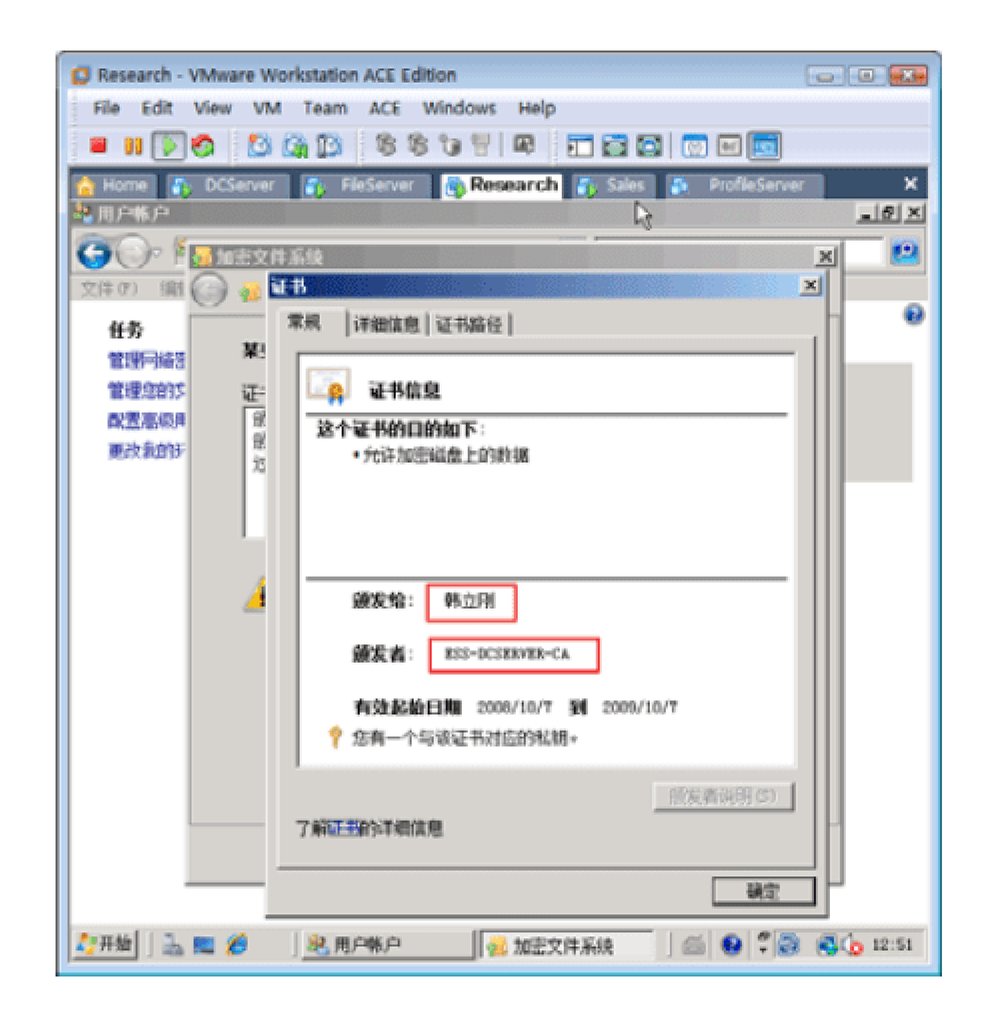


图 6-82　证书的详细信息

㉑ 右击 hanLG EFS 文件夹，在弹出的快捷菜单中选择“共享”命令，在出现的“文件共享”对话框中，单击“共享”按钮。在出现的“用户帐户控制”对话框中输入域管理员账号和密码，如图 6-83 所示。单击“确定”按钮，完成共享。

㉒ 注销韩立刚账户在 Research 上的登录。这样用户的账户配置文件会存储在 FileServer 服务器上的 profiles 文件夹中。

㉓ 使用韩立刚用户账户在Sales计算机上登录，访问Research计算机上的文件夹。双击hanLG test.txt 文件夹，发现能够打开，说明能够解密，如图 6-84 所示。

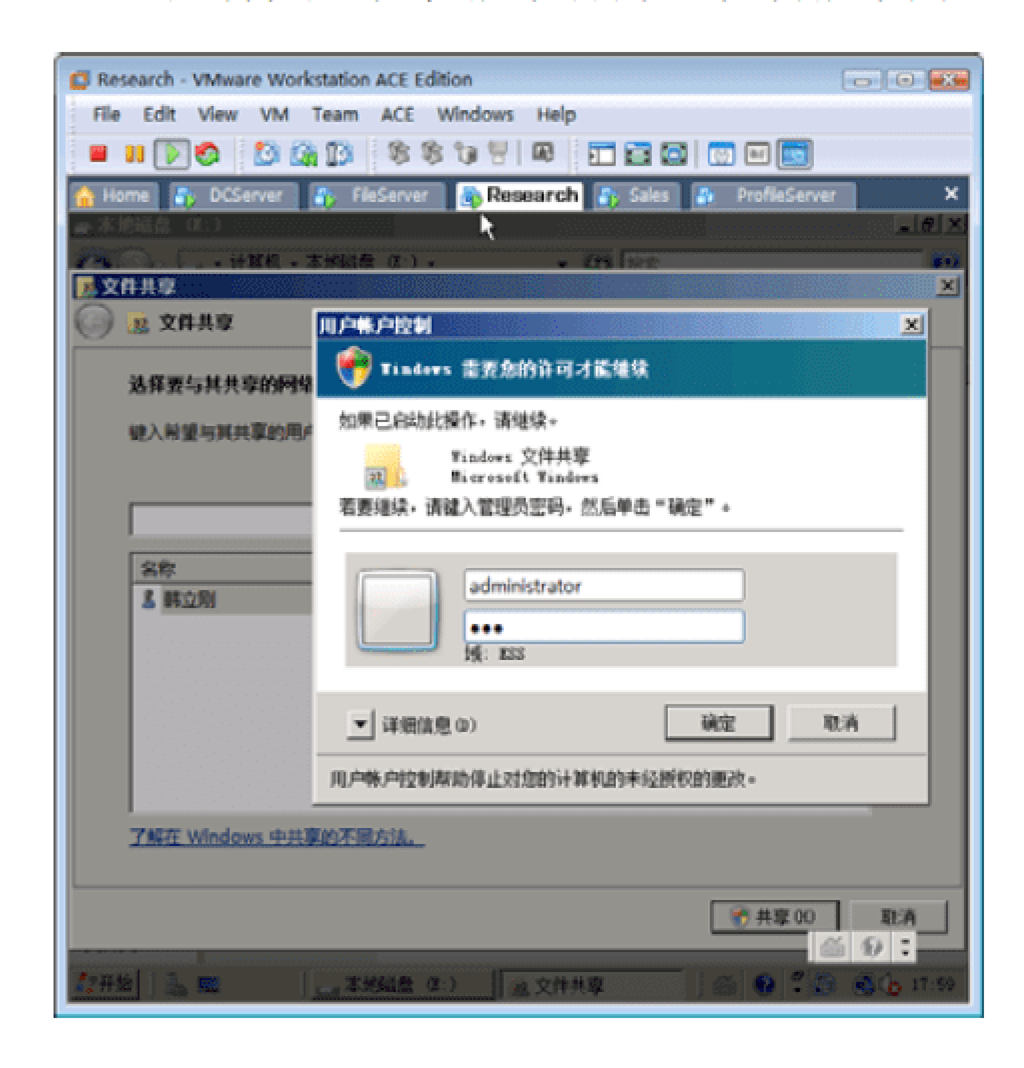


图 6-83　输入管理员账户和密码

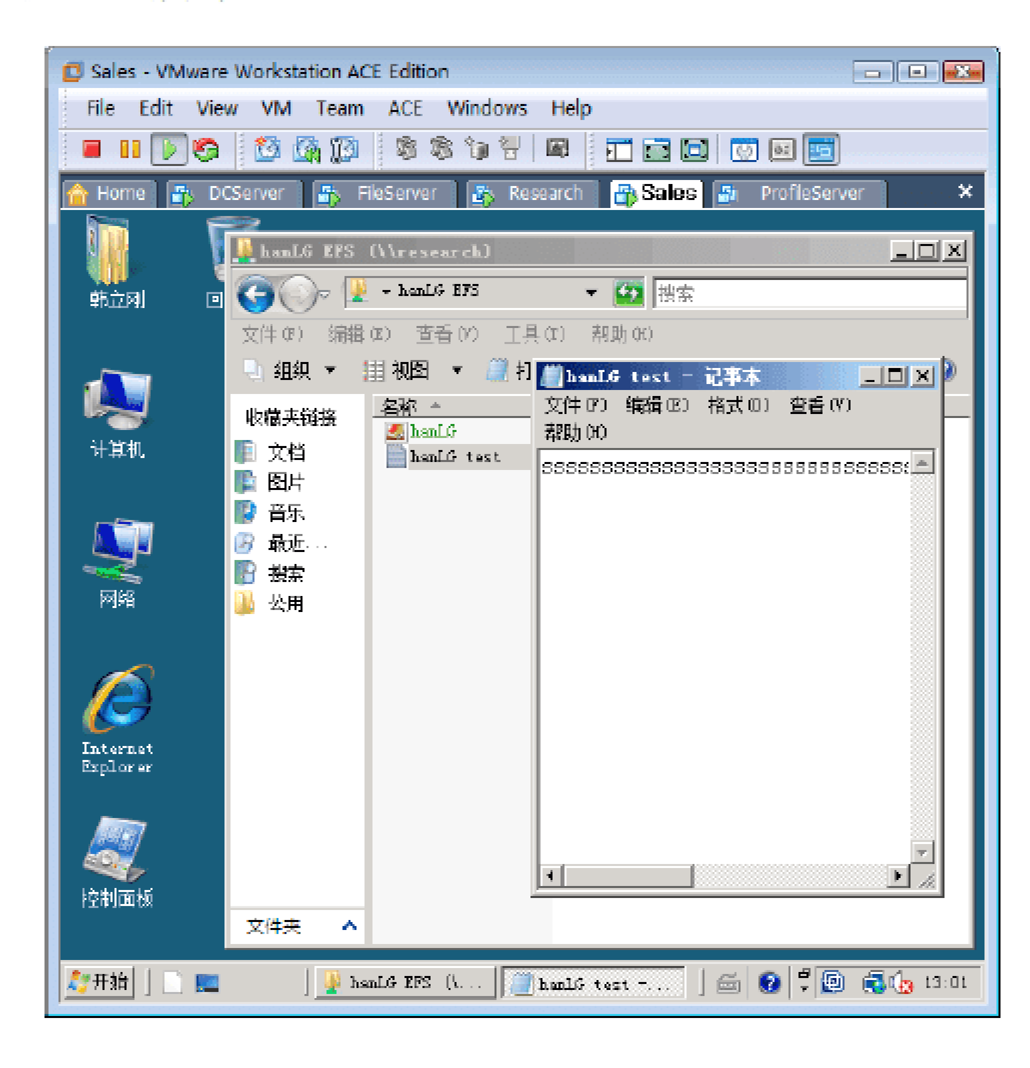


图 6-84　访问网络上的 EFS 能够成功

㉔ 在 DCServer 计算机上以域管理员登录，打开“Active Directory 用户和计算机”窗口，如图 6-85 所示，选择“查看”→“高级功能”命令。

㉕ 如图 6-86 所示，双击“韩立刚”用户账户，在“韩立刚 属性”对话框中，切换到“发布的证书”选项卡，可以看到该用户的证书。

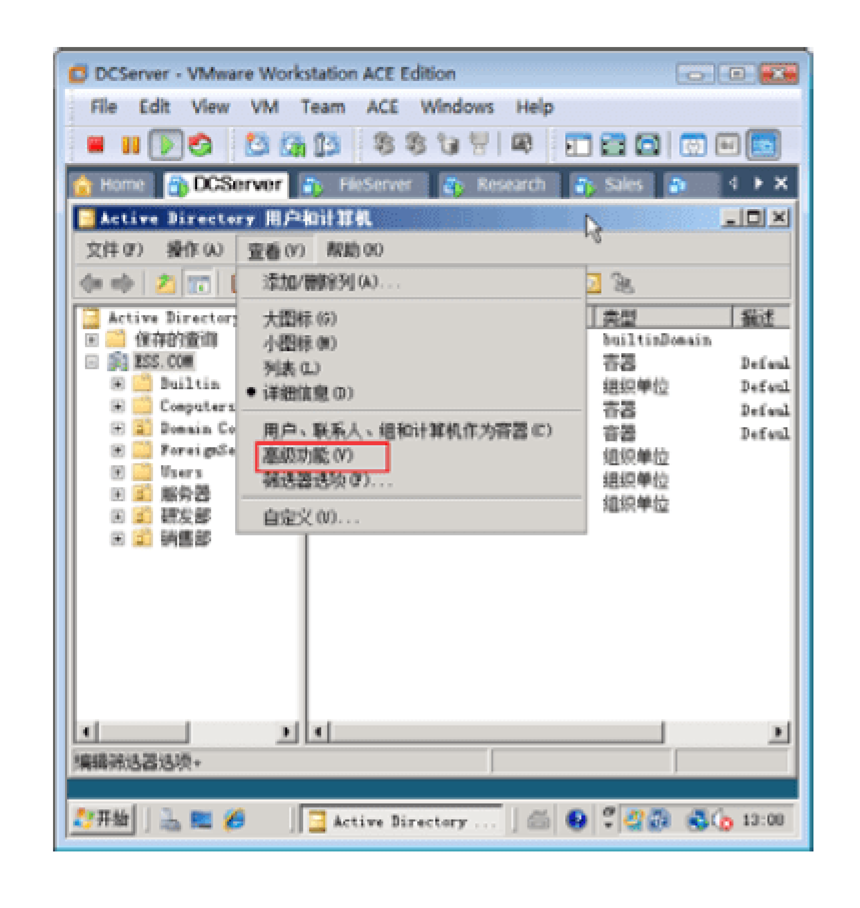



图 6-85　启用高级功能

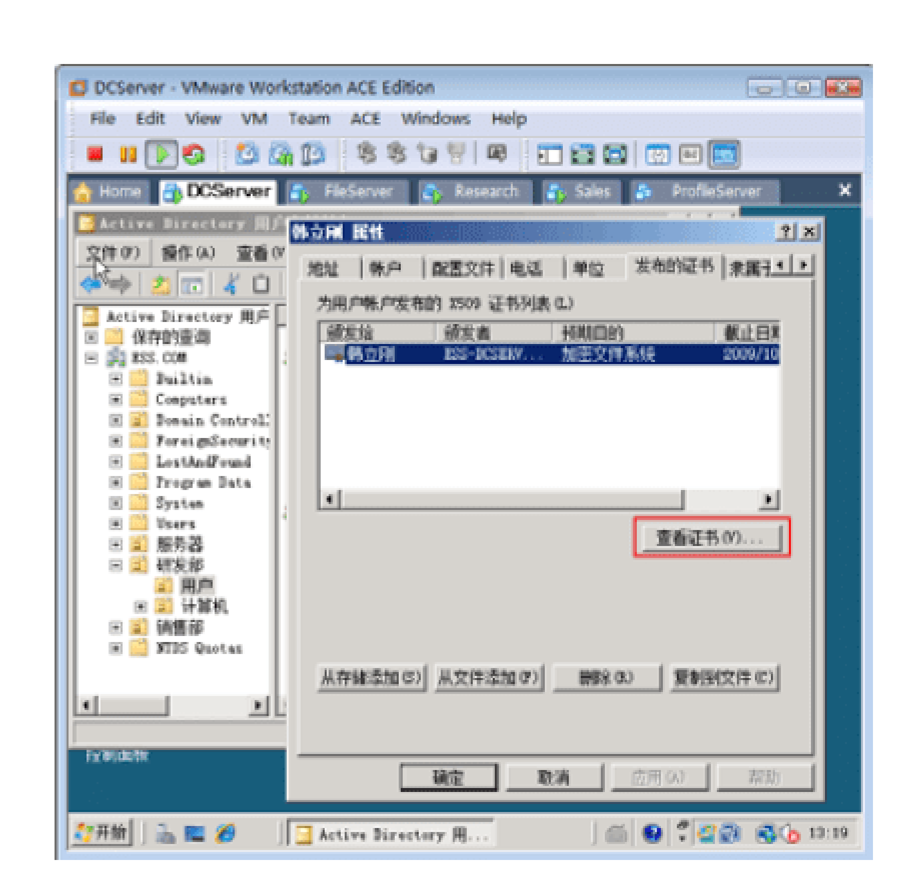


图 6-86　活动目录中存储的 EFS 证书

㉖　如图 6-87 所示，选中该证书，单击“查看证书”按钮，在打开的“证书”对话框中，可以看到该证书没有私钥。


注意：存储在活动目录中的用户证书，只是证书的公钥部分。

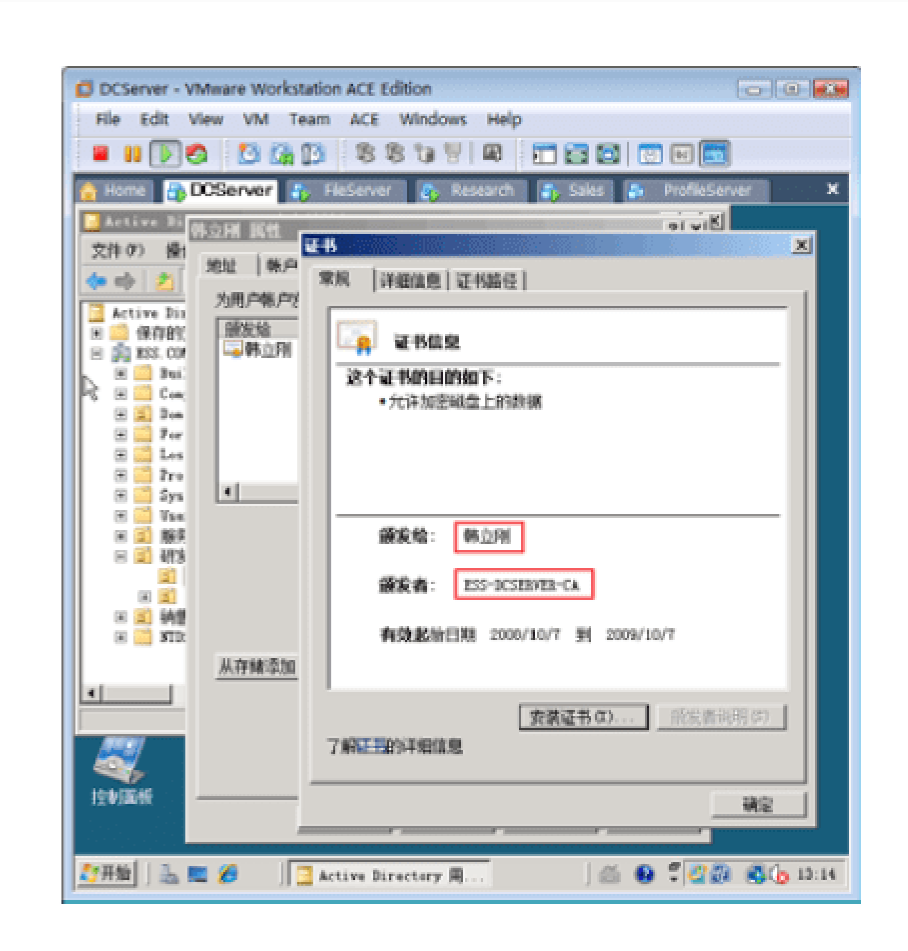


图 6-87　证书的详细信息

6.4.6　指定恢复代理证书

为了防止个别用户账户的 EFS 证书丢失，造成加密的数据不可访问，你可以创建数据恢复代理证书。该用户代理程序可以恢复该部门的或整个域的用户加密的文件。

示例：给域中所有计算机指定一个数据恢复代理证书。

①　以域管理员身份登录 DCServer。

②　选择“开始”→“程序”→“管理工具”→“组策略管理”命令。

③　如图 6-88 所示，在“组策略管理”对话框中，右击 Default Domain Policy 选项，在弹出的快捷

菜单中选择“编辑”命令。



提示：该组策略默认连接在域级别上，因此影响到域中所有的计算机。如果你想对销售部门的计算机指定数据恢复代理证书，你可以创建新的组策略，并将该组策略连接到销售部门的组织单元。

④ 在“组策略管理编辑器”对话框中，如图 6-89 所示，右击“加密文件系统”选项，在弹出的快捷菜单中选择“创建数据恢复代理程序”命令。

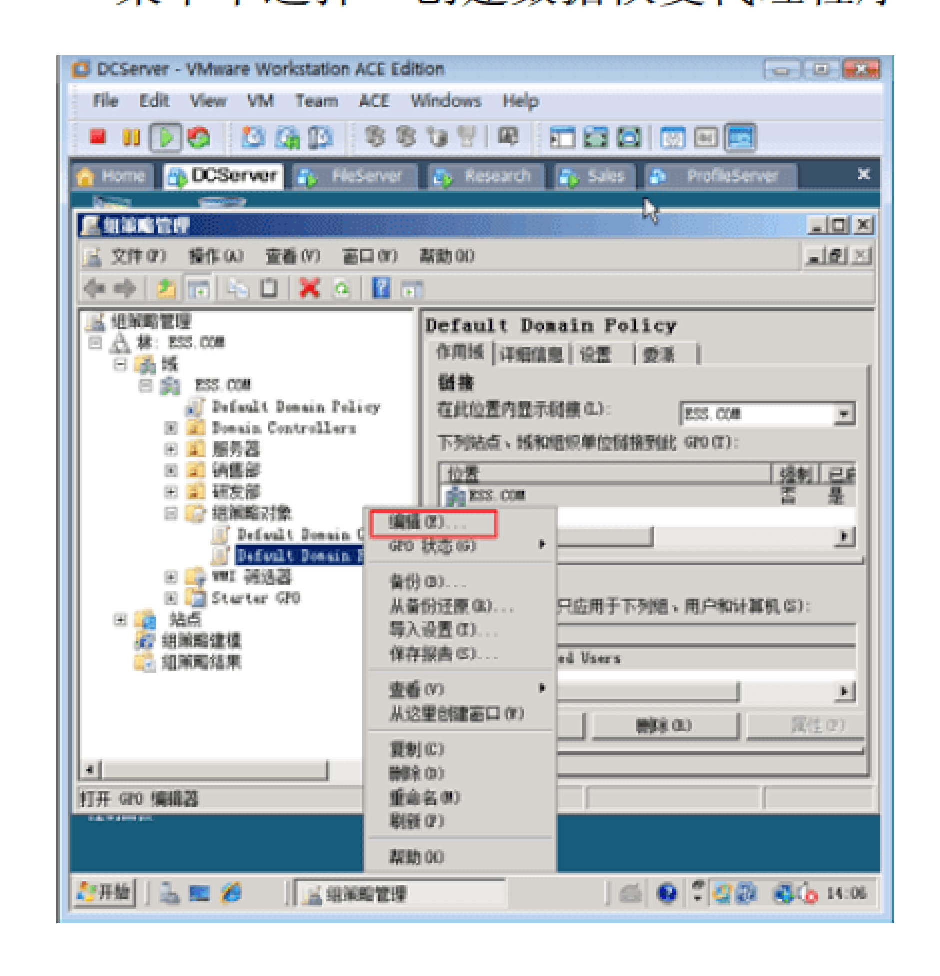


图 6-88　编辑默认域策略

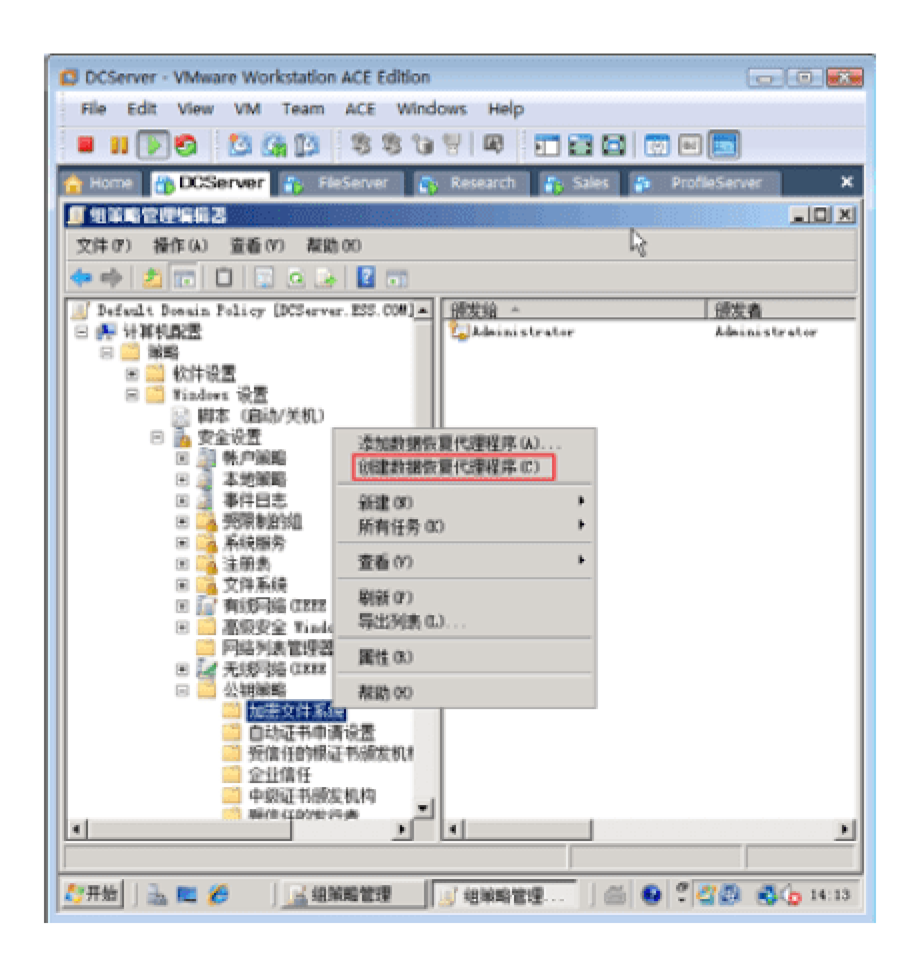


图 6-89　创建数据恢复代理程序

⑤ 如图 6-90 所示，此时会看到 ESS-DCSERVER-CA 发给 Administrator 的文件恢复证书。

⑥ 双击该证书，打开“证书”对话框，如图 6-91 所示，你会看到证书的目的为文件恢复，并且能看到你有一个与该证书对应的私钥。

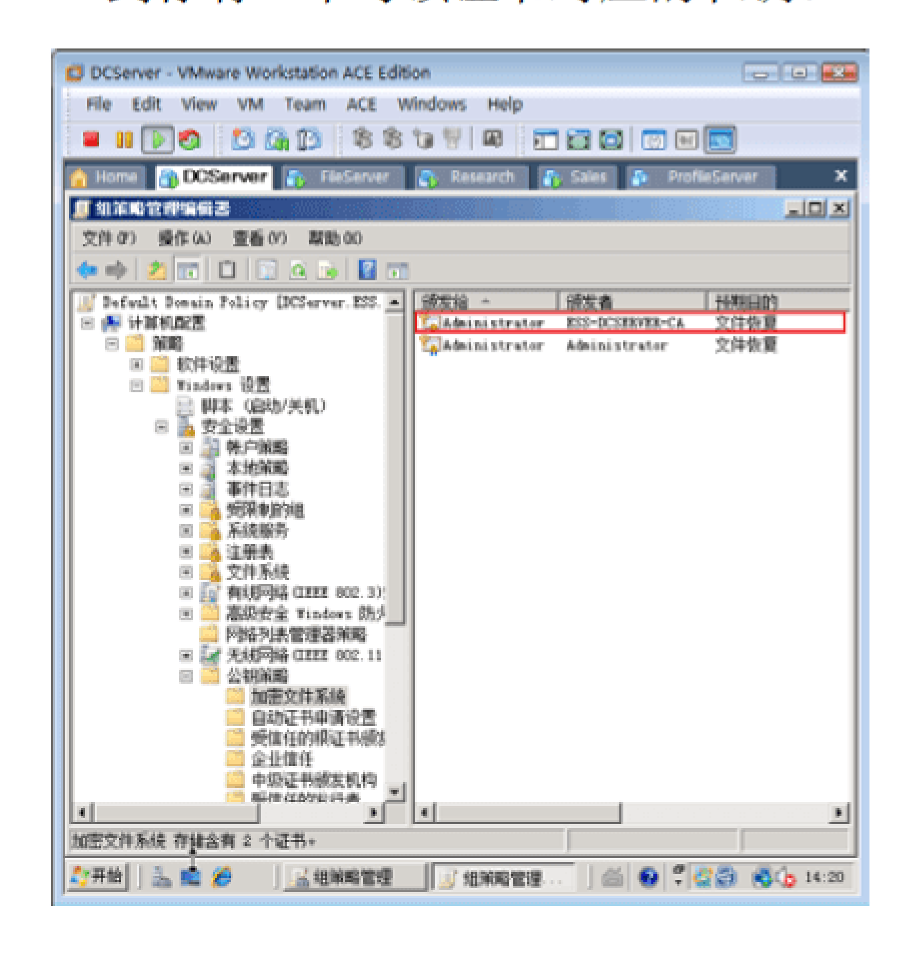


图 6-90　向企业 CA 申请的证书

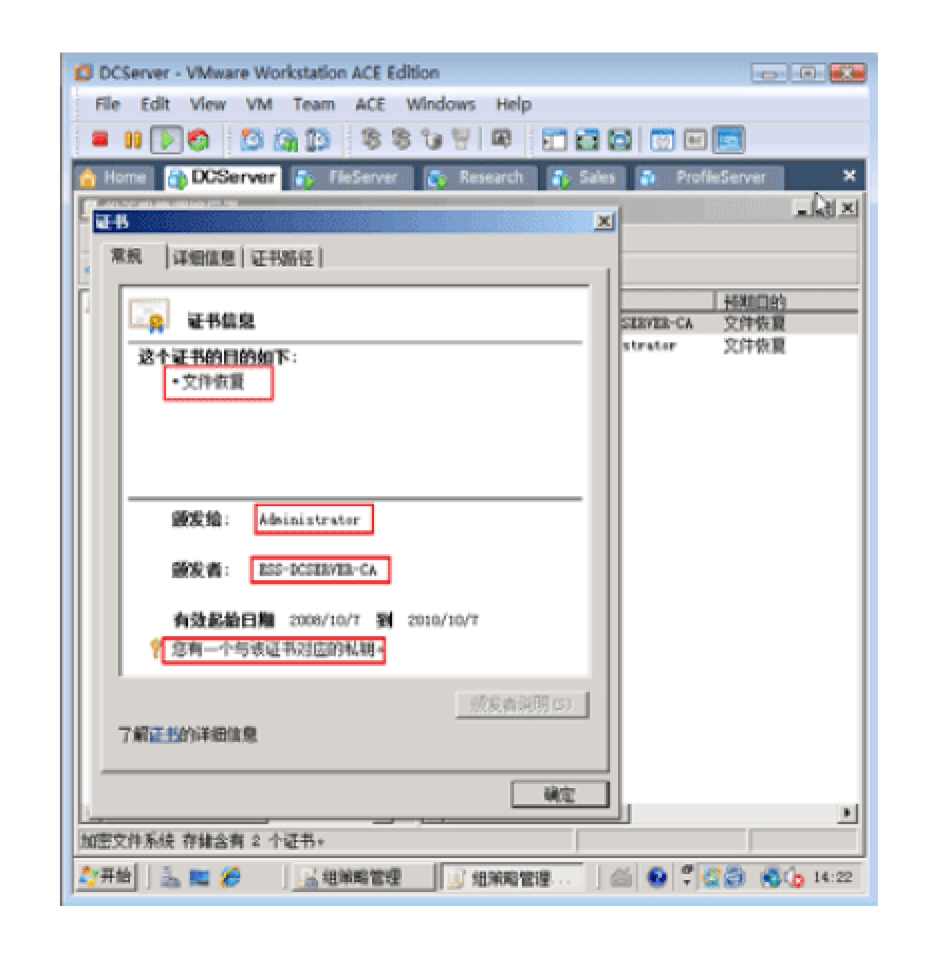


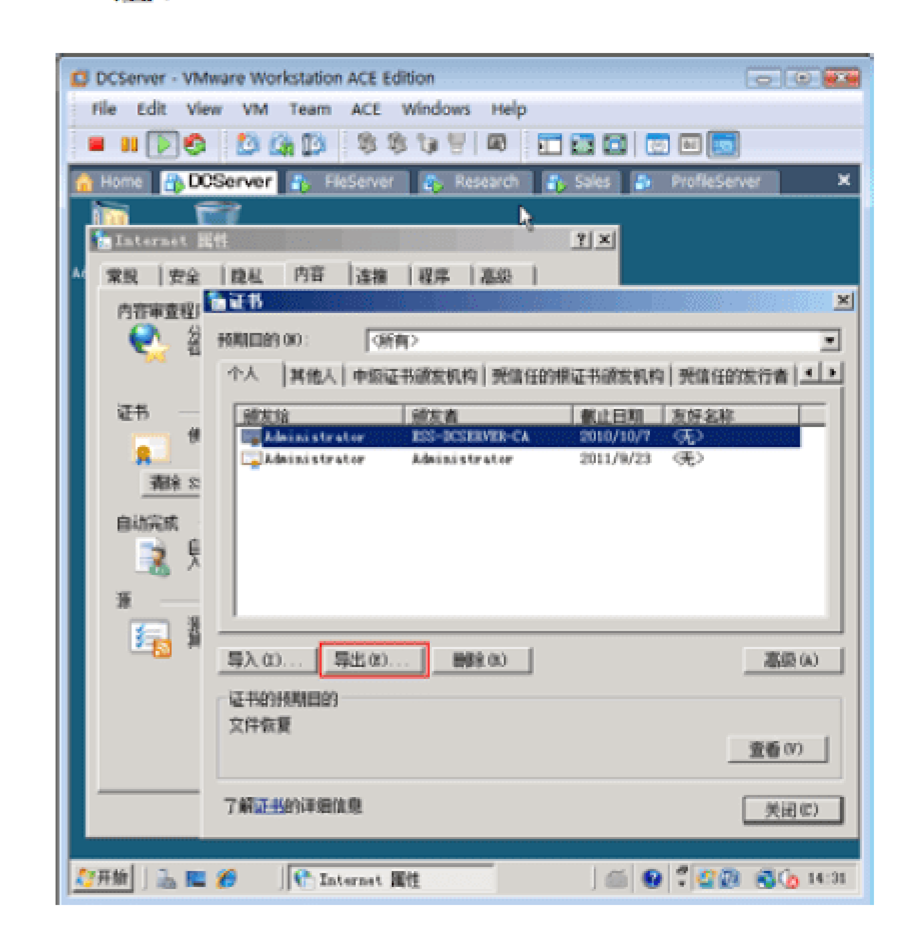
图 6-91　证书的用途和颁发者

⑦ 关闭组策略编辑器。

⑧ 打开 IE 属性对话框，在“内容”选项卡中，如图 6-92 所示，单击“证书”按钮。在打开的“证书”对话框中，选中文件恢复证书，单击“导出”按钮。

⑨ 如图 6-93 所示，在“导出私钥”界面中，选中“是，导出私钥”单选按钮，单击“下一步”按

钮。



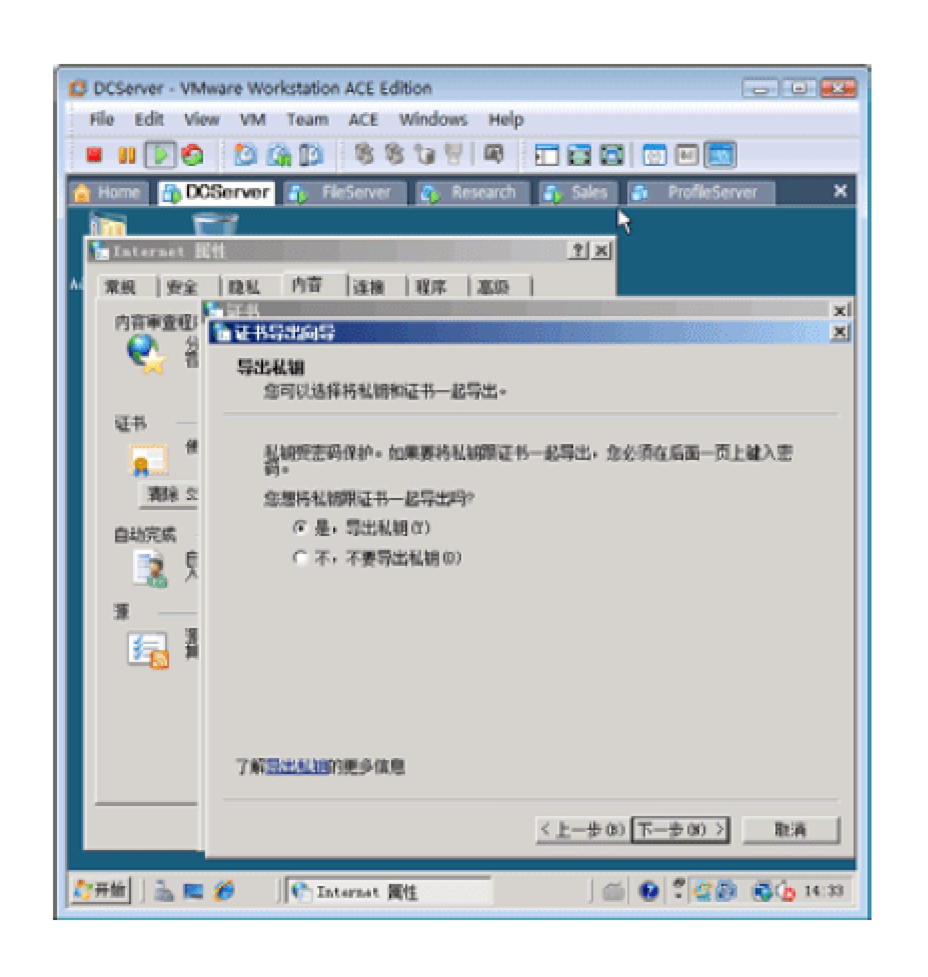




图 6-92　导出恢复代理证书

图 6-93　导出私钥

⑩ 如图 6-94 所示，在出现的“导出文件格式”界面中，单击“下一步”按钮。

⑪ 如图 6-95 所示，在出现的“密码”界面中，输入密码并确认，单击“下一步”按钮。

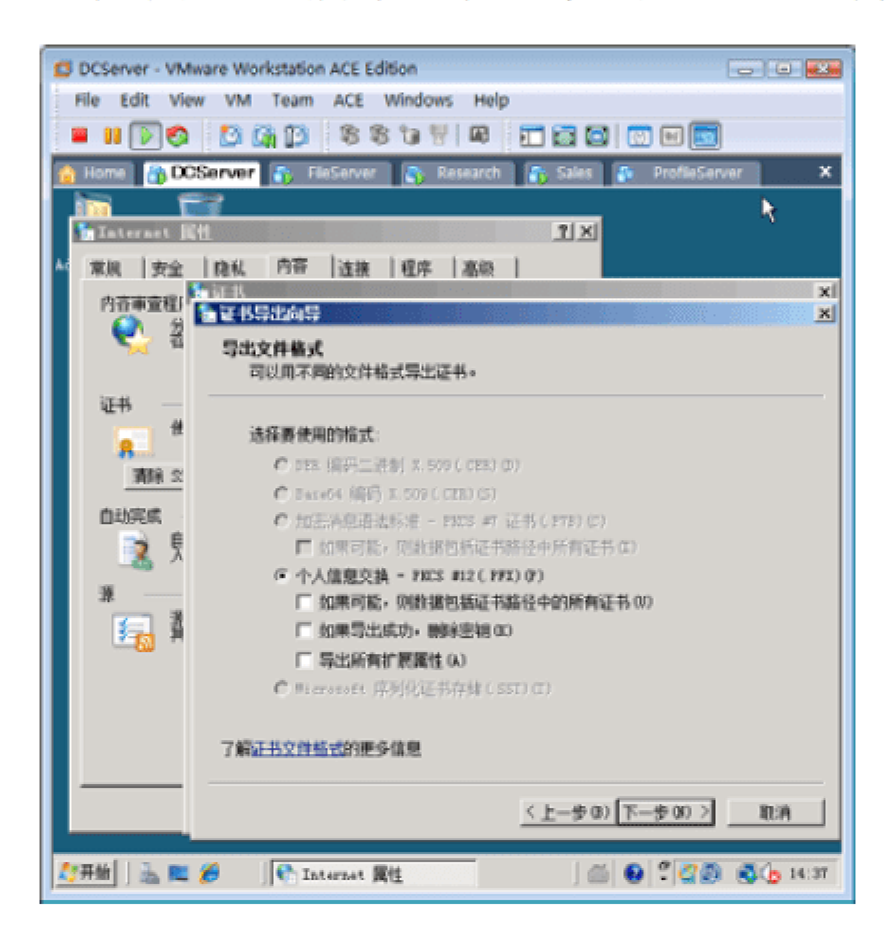


图 6-94　证书格式

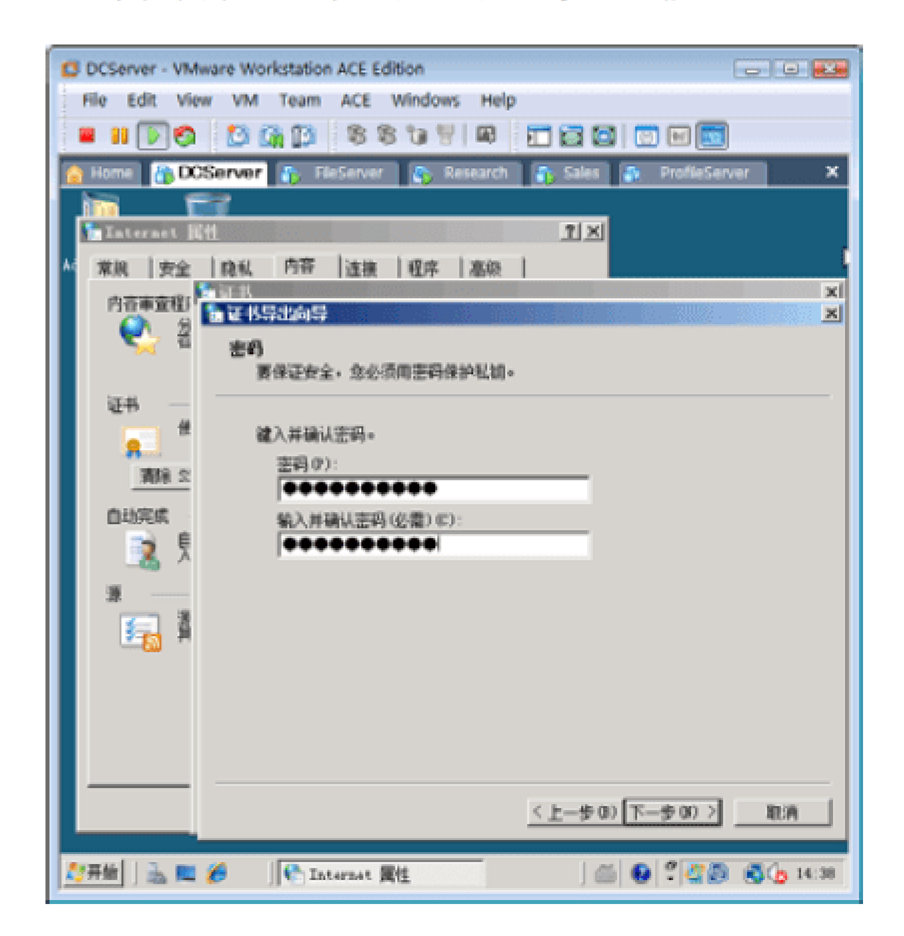


图 6-95　输入密钥

⑫ 如图 6-96 所示，在出现的“要导出的文件”界面中，输入存储证书路径和文件名，单击“下一步”按钮，完成导出。

注意：将导出的恢复代理证书妥善保存起来，为了安全起见，现在你可以删除存储在域控制器上的恢复代理证书了。

⑬ 如图 6-97 所示，在 Research 计算机上运行 gpupdate /force，强制刷新组策略。

⑭ 在 hanLG EFS 文件夹中创建一个记事本文件 second test.txt。

⑮ 切换用户，以域管理员登录 Research，双击 Second test.txt 文件，你将会发现拒绝访问。

⑯ 从 DCServer 计算机上将恢复代理证书复制到 Research 计算机。打开 IE 属性对话框，切换到“内容”选项卡，单击“证书”按钮。

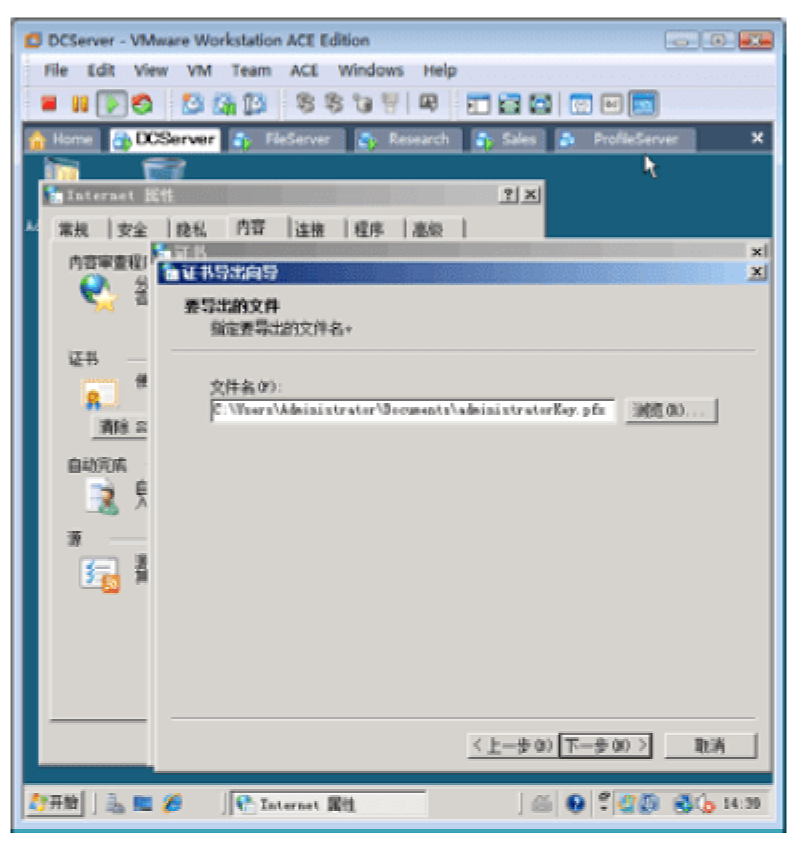




图 6-96　指定保存位置

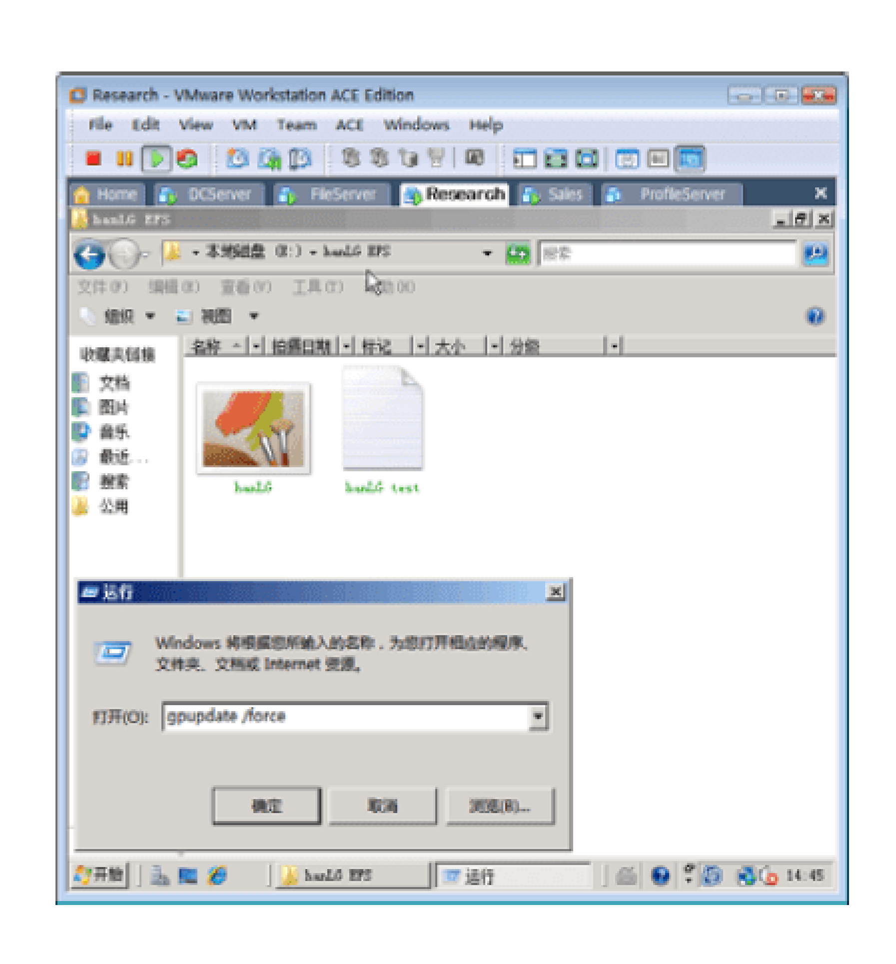


图 6-97　强制刷新组策略

⑰　在如图 6-98 所示的“证书”对话框中，浏览到恢复代理证书，单击“导入”按钮，单击“下一步”按钮，在打开的“密码”对话框中，输入密码，将恢复代理证书导入。

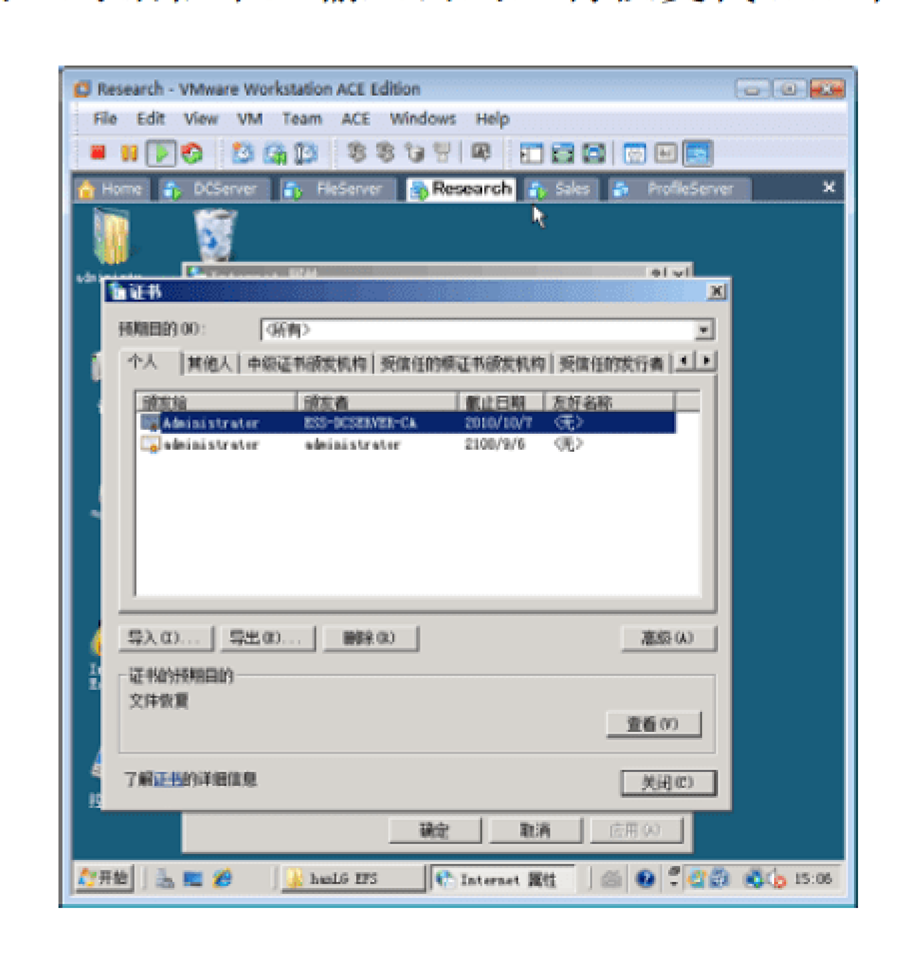


图 6-98　导入恢复代理证书

⑱　双击 second test.txt 文件，能够打开。

⑲　双击 hanLG test.txt 文件，提示拒绝访问。



提示：恢复代理证书只能解密那些指定恢复代理证书的组策略应用以后的加密文件，因此不能解密 hanLG test.txt 文件。

6.4.7　应该在何时加密文件和文件夹

如果你认为文件或文件夹拥有 Windows 可以提供的最强保护措施这一点非常重要，则应当对这些文件或文件夹进行加密。由于加密文件和文件夹非常容易，因此可以尝试加密所有的信息，但是应记住下面这些事项。

- 需要确保备份你的加密证书和加密密钥，并将其保存在安全的位置。如果加密证书和密钥丢失或损坏，你将无法再使用已加密的文件。如果加密一个文件夹，则在该文件夹中创建的所有文件都将被自动加密。
- 其他想要访问已加密的文件或文件夹的用户必须将其自己的加密文件系统（EFS）证书添加到这些文件中。通过此证书，他们在你的计算机上工作时即可访问加密的文件或文件夹。如果文件已共享，他们可以从另一台运行 Windows 的计算机上访问这些文件。
- 如果将某个文件复制或移动到不使用 NTFS 文件系统的计算机或卷，该文件将被解密。

6.4.8 移动或复制对加密状态的影响

你可以将自己加密的文件或文件夹移动或复制到其他目录，移动和复制操作对加密状态的影响，分以下几种情况。

- 将文件或文件夹复制或移动到加密状态的文件夹，将会自动变成加密状态。
- 将加密的文件或文件夹复制或移动到其他 NTFS 分区，加密状态不变。
- 将加密的文件或文件夹复制或移动到 FAT32 分区，文件变成不加密状态。

6.4.9 用户密码重设对 EFS 的影响

由管理员重置用户密码或使用其他工具重设计算机本地用户密码后，EFS、凭据和证书私钥将不可用。你可能会失去给用户的访问权限。


注意：域用户不存在这个问题，也就是说域用户的密码如果忘了，可以找域管理员重新设置新的密码。

- Web 页凭据。
- 存储的网络密码。
- EFS 加密文件。
- 证书与私钥（签名/加密电子邮件）。

若要恢复所有数据，你必须具备下列条件之一。

- 原始密码。这是当用户上次成功登录并能够访问他们的凭据和文件时的密码。
- 密码故障恢复磁盘（PRD）。必须在用户具有访问文件权限时创建的密码恢复磁盘。

示例：密码重设后 EFS 不可解密。

本示例演示将 Research 计算机上本地用户“张帅”的密码由 p@ssw0rd 重设成 p@ssw0rd01 后，加密的文件不能访问。

① 以 Research 计算机上本地管理员登录，创建一个“张帅”用户账户，登录名为 zhangS，密码为 p@ssw0rd，如图 6-99 所示。
② 以“张帅”账户登录 Research 计算机。
③ 创建一个文件夹 zhangS EFS，并将该文件夹设置成加密状态。
④ 在该文件夹中创建一个记事本文件。
⑤ 注销“张帅”用户。

⑥　以 Research 计算机本地管理员登录，右击“张帅”用户账户，在弹出的快捷菜单中选择“设置密码”命令，在出现的“为 ZhangS 设置密码”对话框中，单击“继续”按钮，如图 6-100 所示。

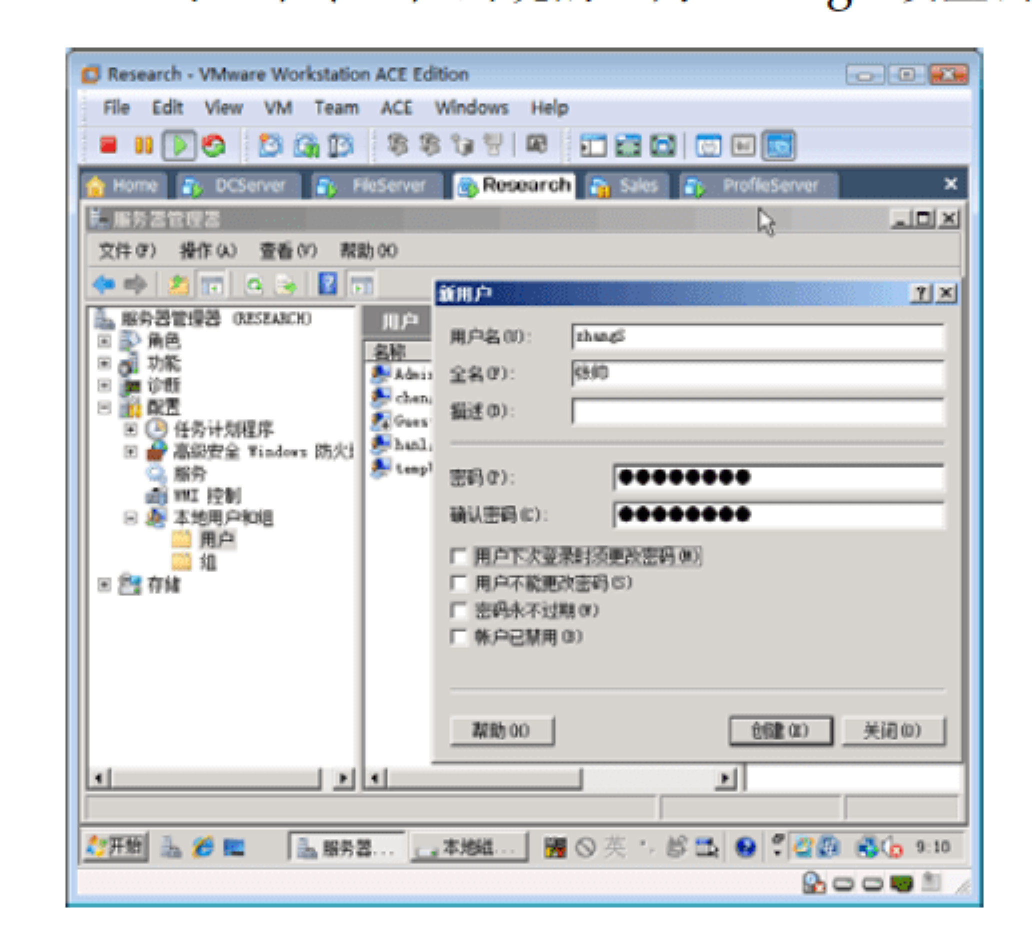



图 6-99　创建一个新用户

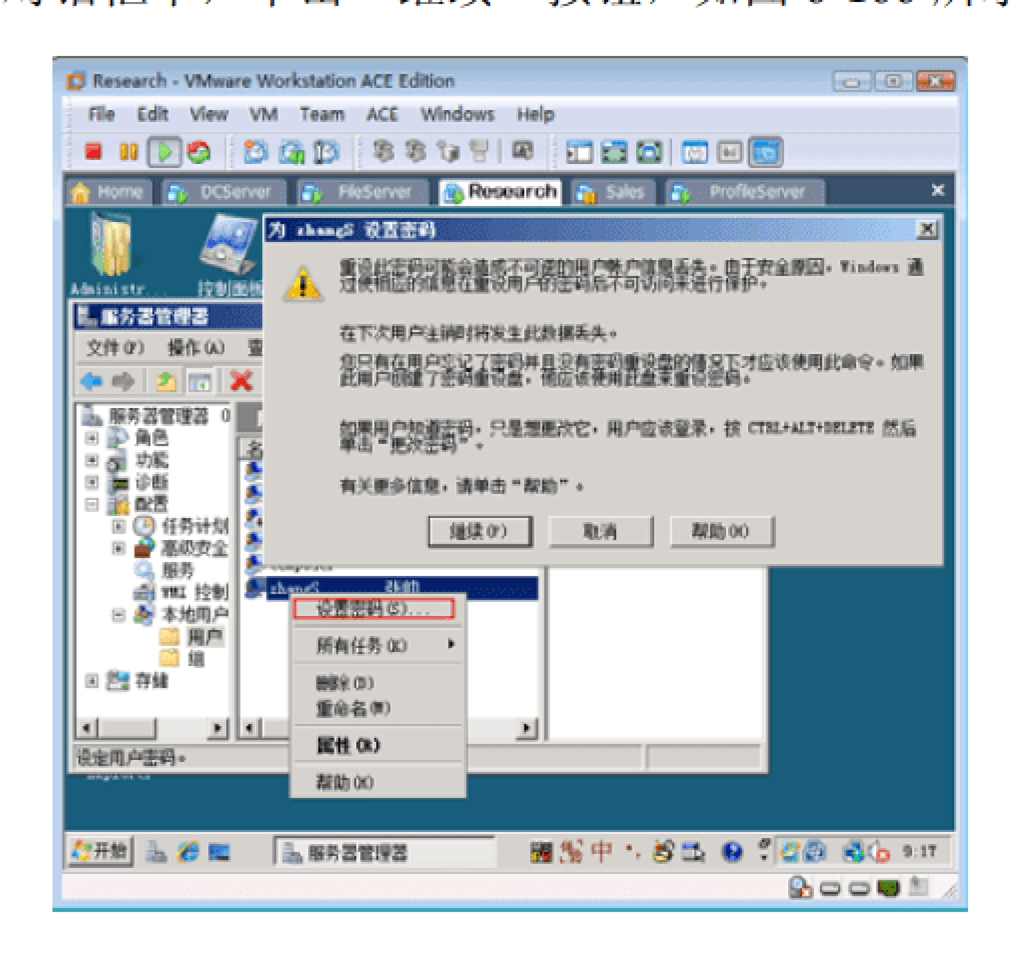


图 6-100　重设密码时的提示



提示：“重设此密码可能会造成不可逆的用户账户信息丢失。出于安全原因，Windows 通过相应的信息在重设用户的密码后不可访问来进行保护。在下次用户注销时将发生此数据丢失。你只有在用户忘记了密码并且没有密码重设盘的情况下才可以使用此命令。如果此用户创建了密码重设盘，他应该使用磁盘来重设密码。如果用户知道密码，只是想更改它，用户应该登录，按 Ctrl+Alt+Del 组合键，然后单击“更改密码”按钮。

⑦　在出现的重设密码对话框中，输入新密码 p@ssw0rd01，单击“确定”按钮。

⑧　注销管理员，以“张帅”的账户登录 Research。

⑨　双击加密的文件，系统提示“拒绝访问”，如图 6-101 所示。

⑩　按 Ctrl+Alt+Del 组合键，单击“更改密码”按钮。输入旧密码 p@ssw0rd01，新密码 p@ssw0rd。单击按钮，将密码更改为加密时的密码。

⑪　再次双击加密的文件，成功打开，如图 6-102 所示。

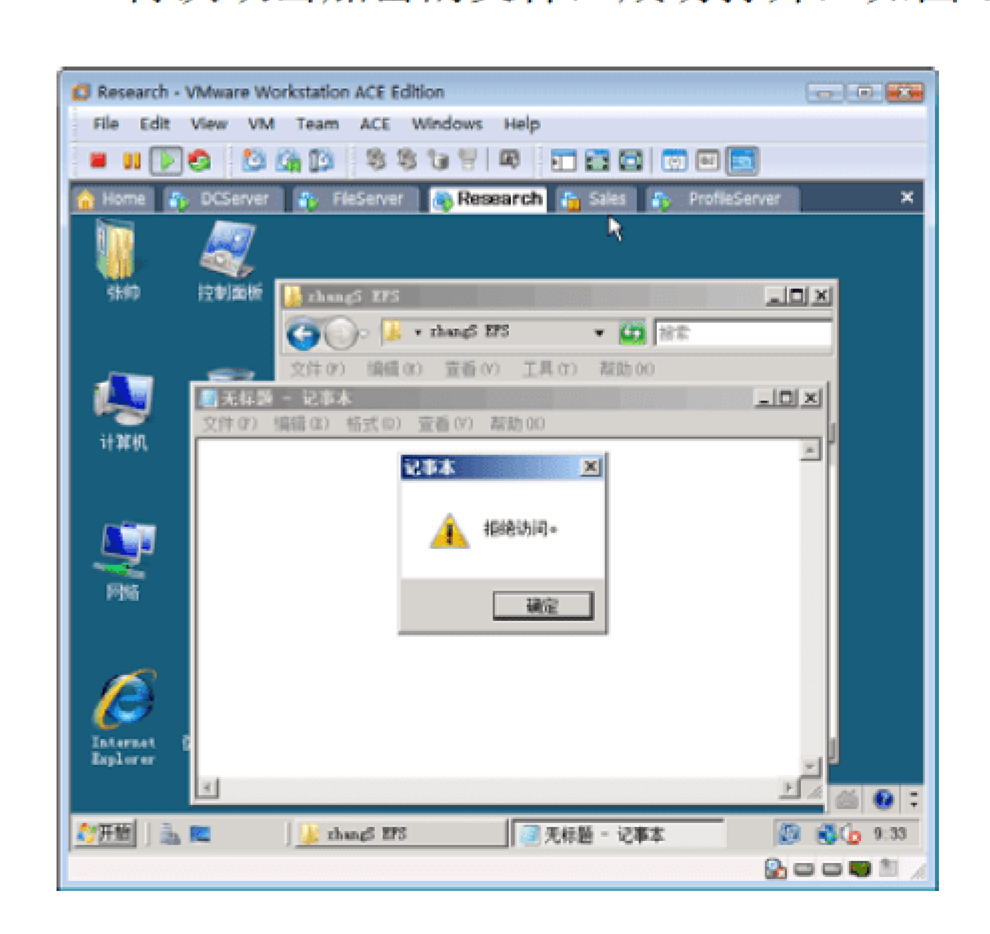


图 6-101　重设密码后不能解密以前加密的文件

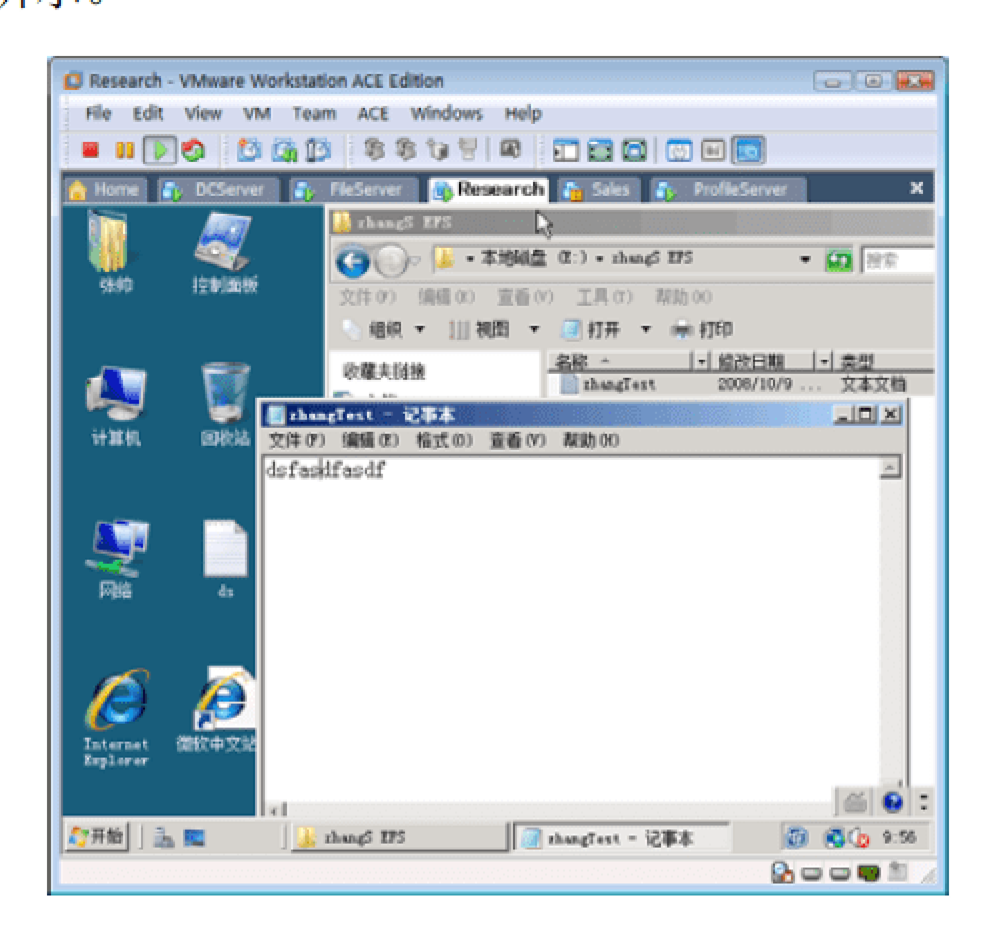


图 6-102　更改回原来的密码后就能解密



注意：如果加入域后的计算机，默认的安全策略不允许立即更改密码，在更改密码时会提示不符合密码策略。可以在 DCServer 计算机上修改组策略，允许用户能够立即更改密码。

6.5 压　　缩

可以对文件、文件夹或整个卷进行压缩。NTFS 文件系统的压缩过程和解压过程对用户是完全透明的，压缩前和压缩后的文件在使用上没有不同。

说明

- 当把一个未压缩的文件或文件夹复制到一个压缩的文件夹或卷中时，会自动压缩。
- NTFS 压缩和 EFS 加密不能同时使用，所以对于需要加密的文件或文件夹不要压缩。
- 在同一个 NTFS 卷中，当把一个压缩的文件或文件夹复制到一个未压缩的文件夹或卷中时，其状态仍为压缩。
- 在不同 NTFS 卷间，当把一个压缩的文件或文件夹复制到一个未压缩的文件夹或卷中时，会自动解压。
- 当一个压缩的文件从 NTFS 卷移动或复制到 FAT 卷时将自动解压。

6.5.1 压缩文件夹

你可以将不常用的文件放到设置成压缩状态的文件夹中。

示例：启用对文件夹的压缩。

① 在 Research 计算机上创建一个“安装文件”文件夹，在“安装文件”文件夹中创建一个图片文件 photo.bmp，单击“编辑”按钮，随便画一些内容，保存。

② 右击该文件夹，在弹出的快捷菜单中选择“属性”命令，打开文件属性对话框。在“常规”选项卡中，单击“高级”按钮，在“高级属性”对话框中，选中“压缩内容以便节省磁盘空间”复选框，单击“确定”按钮，如图 6-103 所示。

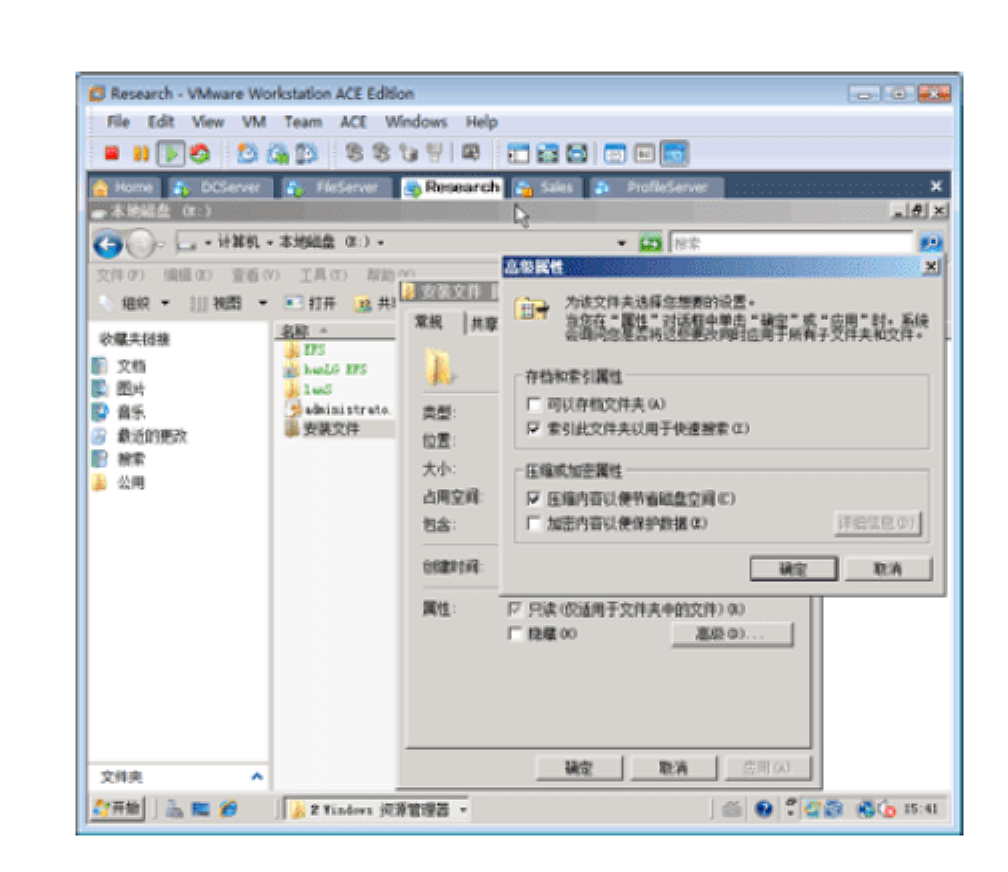


图 6-101　压缩文件夹

③ 打开如图 6-104 所示的对话框，选中“将更改应用于此文件夹，子文件夹和文件”单选按钮。单击“确定”按钮。

④ 如图 6-105 所示，右击“安装文件”文件夹，在弹出的快捷菜单中选择“属性”命令打开该文件的属性对话框。切换到“常规”选项卡，查看文件的大小和占用的空间。

注意：你不能同时选择压缩和加密。观察压缩的文件夹变成了蓝色。

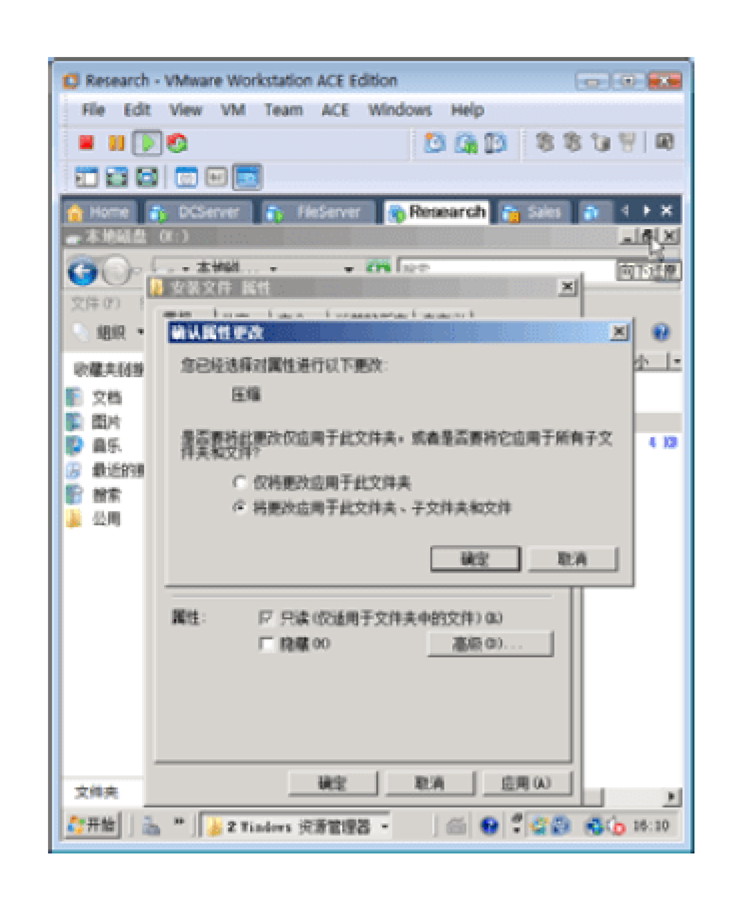


图 6-104　压缩子文件夹和文件

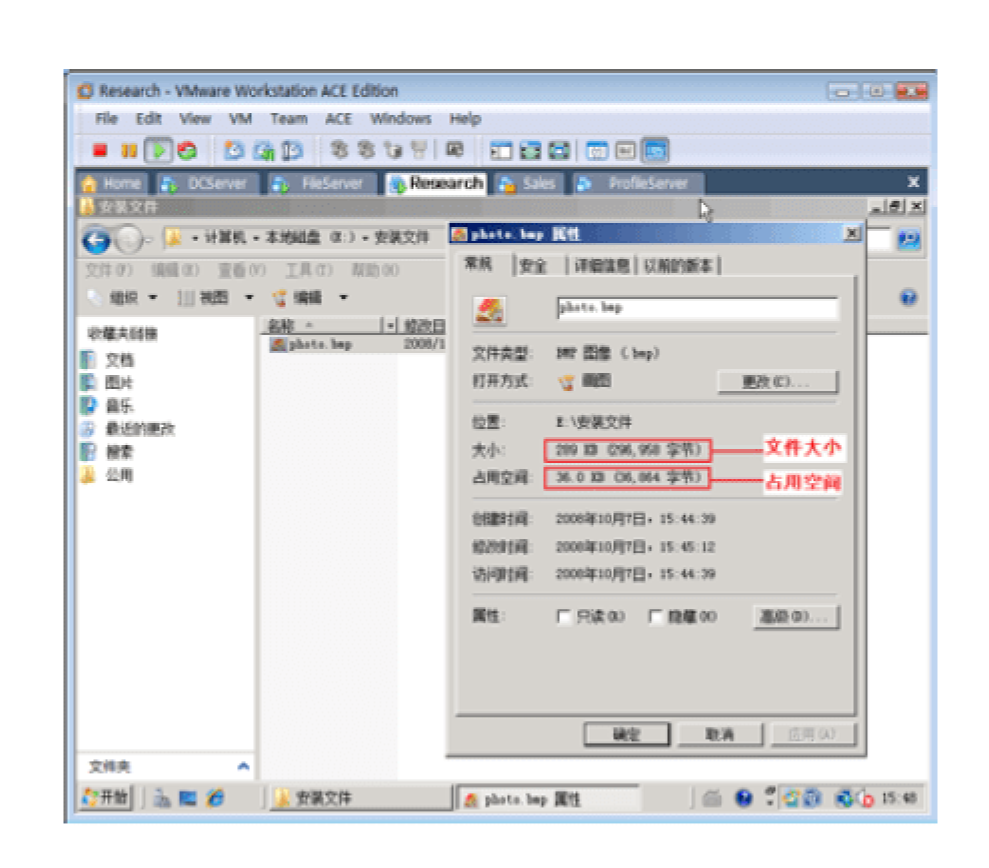


图 6-105　压缩后文件的实际大小和占用空间

6.5.2　压缩整个磁盘

你可以将整个 NTFS 分区的磁盘设置成压缩状态。



注意：如果将整个磁盘分区设置成压缩状态，该磁盘分区不能有加密的文件夹和文件。

示例：将磁盘分区设置压缩状态。

① 右击磁盘分区，在弹出的快捷菜单中选择“属性”命令。

② 在磁盘属性对话框的“常规”选项卡中，选中“压缩此驱动器以节约磁盘空间”复选框，如图 6-106 所示，单击“确定”按钮。

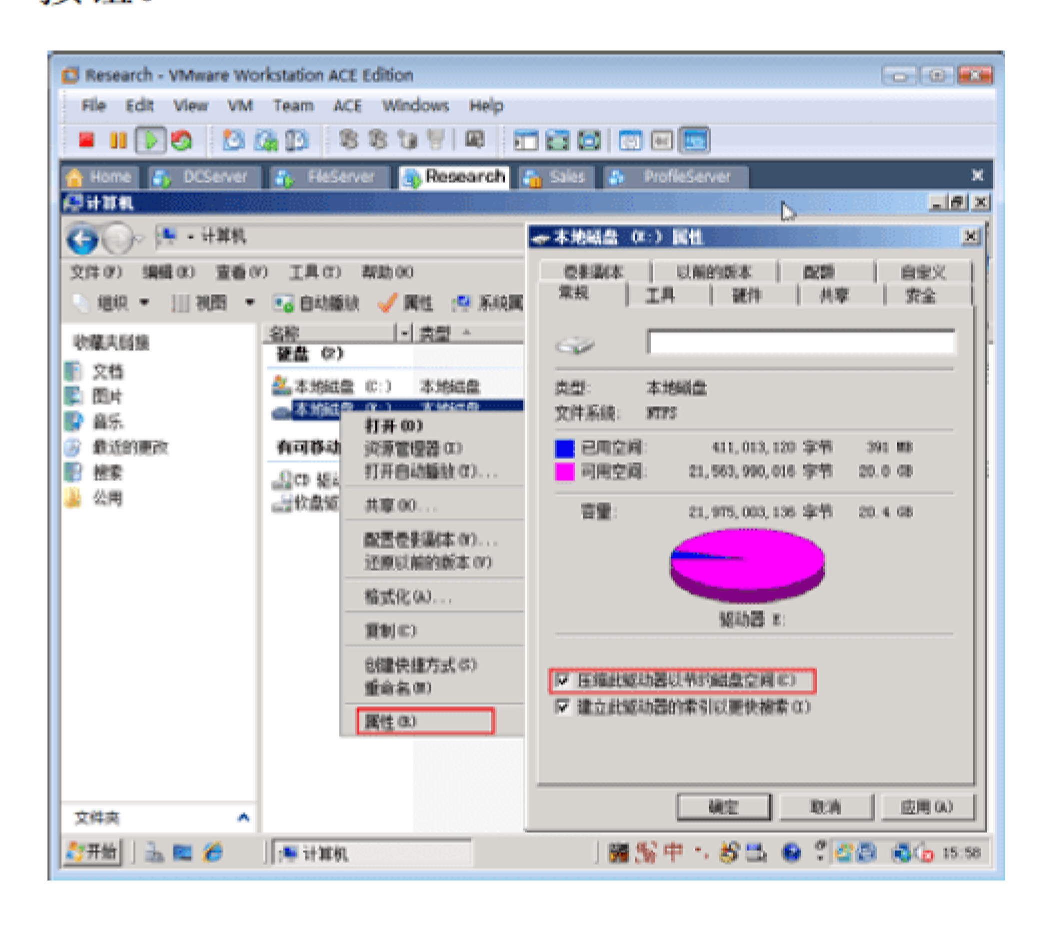


图 6-106　压缩整个磁盘

6.5.3　移动或复制对压缩状态的影响

只有在文件夹中创建新文件或文件夹时才继承目标文件夹的压缩状态。同分区移动，文件或文件夹没

有改变在磁盘上的存储位置，只是改变了文件的访问路径，因此不继承目标文件夹的状态；不同分区移动，实际上是复制文件或文件夹到新位置后删除源文件的过程，因此继承目标文件夹的压缩状态。

这里共有三种情况，同一 NTFS 分区、不同 NTFS 分区以及 FAT 分区，如表 6-2 所示。

表 6-2　移动或复制对压缩状态的影响

	同一 NTFS 分区	不同 NTFS 分区	FAT 分区
复制	继承目标文件(夹)压缩状态	继承目标文件(夹)权限	压缩状态丢失
移动	保留源文件(夹)压缩状态	继承目标文件(夹)压缩状态	压缩状态丢失

6.6　磁 盘 限 额

文件服务器是支持多用户使用的，使用磁盘限额可以为文件服务器的磁盘指定每个账户用多大磁盘空间，这样可以避免某个用户把磁盘空间耗完。

6.6.1　给所有用户设置统一的磁盘配额

示例：在 FileServer 上实现磁盘限额。

① 以域管理员身份登录 FileServer 计算机。

② 双击“计算机”图标，右击“磁盘”，在弹出的快捷菜单中选择“属性”命令，如图 6-107 所示，切换到“配额”选项卡。

③ 分别选中“启用配额管理”和“拒绝将磁盘空间给超过配额限制的用户”复选框，将磁盘空间限制为 500MB。警告等级设置为 450MB。单击“确定”按钮。

注意：磁盘配额默认对管理员不起作用。

④ 注销管理员，以韩立刚用户账户登录。如图 6-108 所示，双击桌面上的“计算机”图标，打开“计算机”窗口可以看到 E 分区大小为 499MB。在 E 分区属性对话框中，可以看到这个用户的可用空间和已用空间。

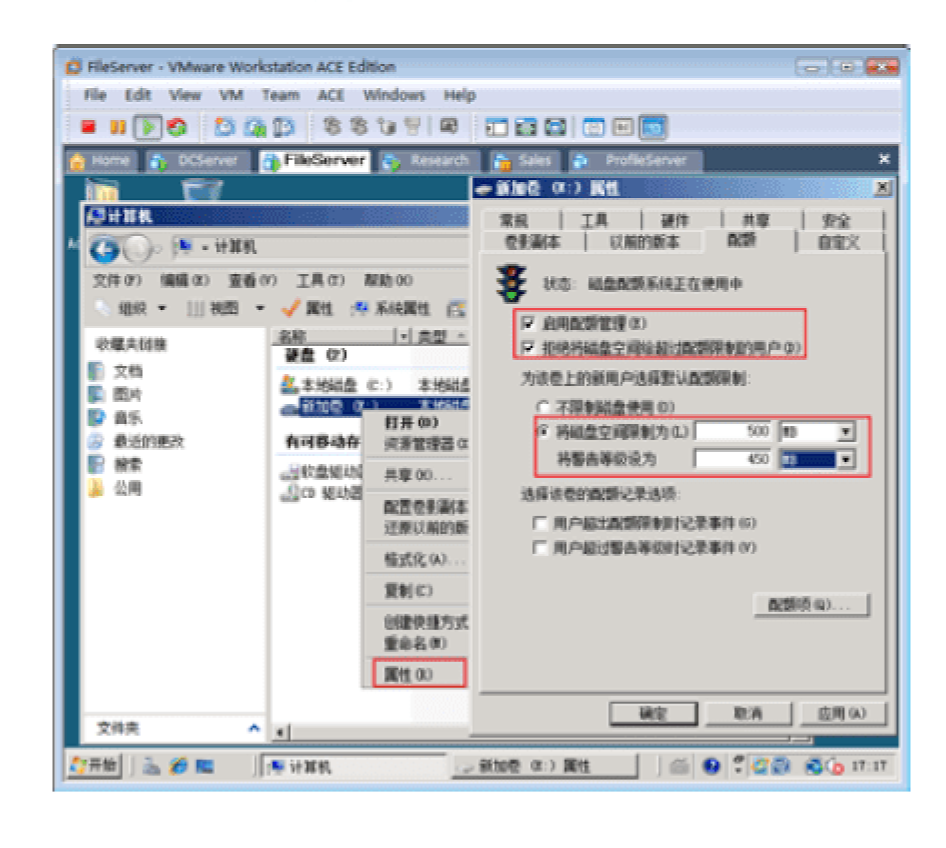


图 6-107　启用磁盘配额

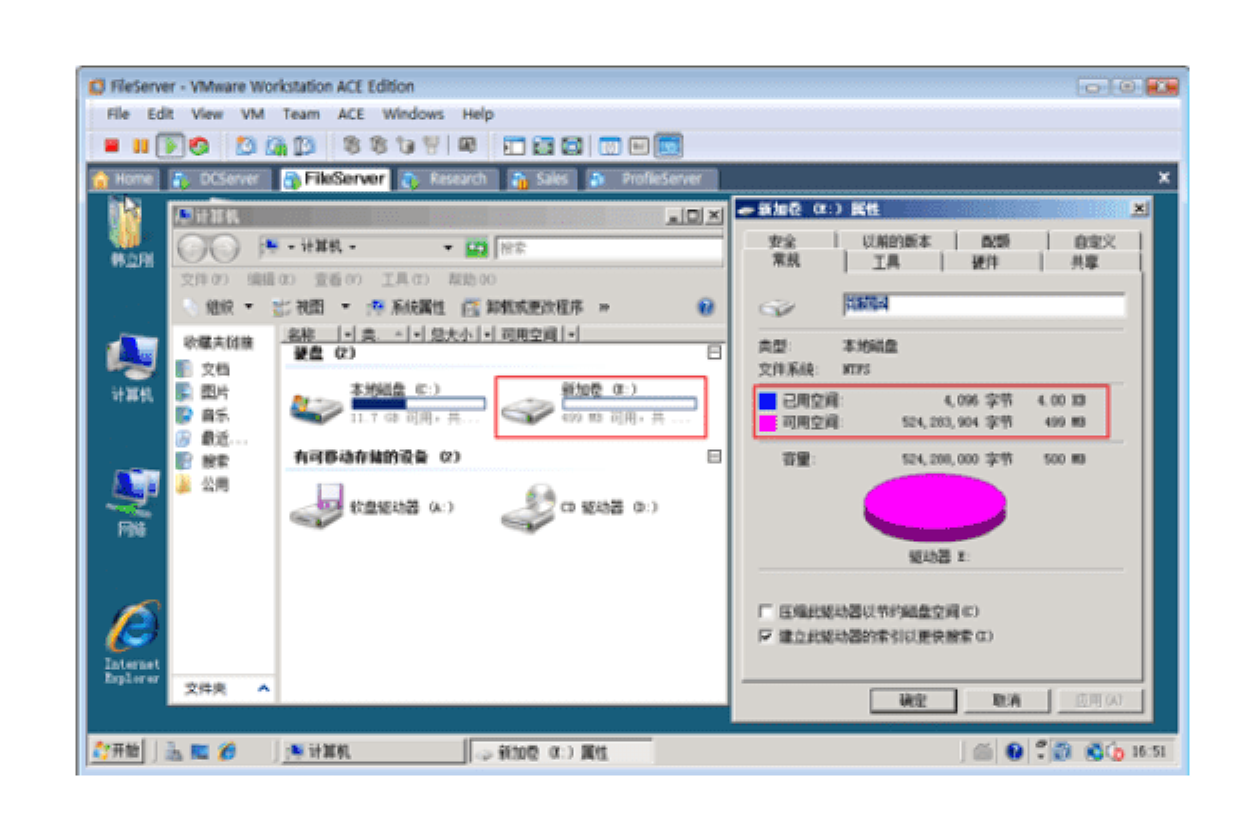


图 6-108　确认磁盘配额



提示：用户的已用空间是根据文件的所有者来计算每个用户的已用空间的。如果有压缩的文件或文件夹，其已用空间是用未压缩状态来计算的。

6.6.2 给个别用户设置特定大小的磁盘配额

设置完磁盘配额后，可能需要给某特定的用户账户指定特定大小的配额。

示例：给韩立刚用户账户指定 1GB 的磁盘限额。

① 以域管理员登录 FileServer，在 E 分区属性对话框的“配额”选项卡中，单击“配额项”按钮。



提示：注意观察 Administrators 组无限制。

② 双击“韩立刚”账户，在随后打开的对话框中可以设置该用户账户的磁盘配额，如图 6-109 所示。

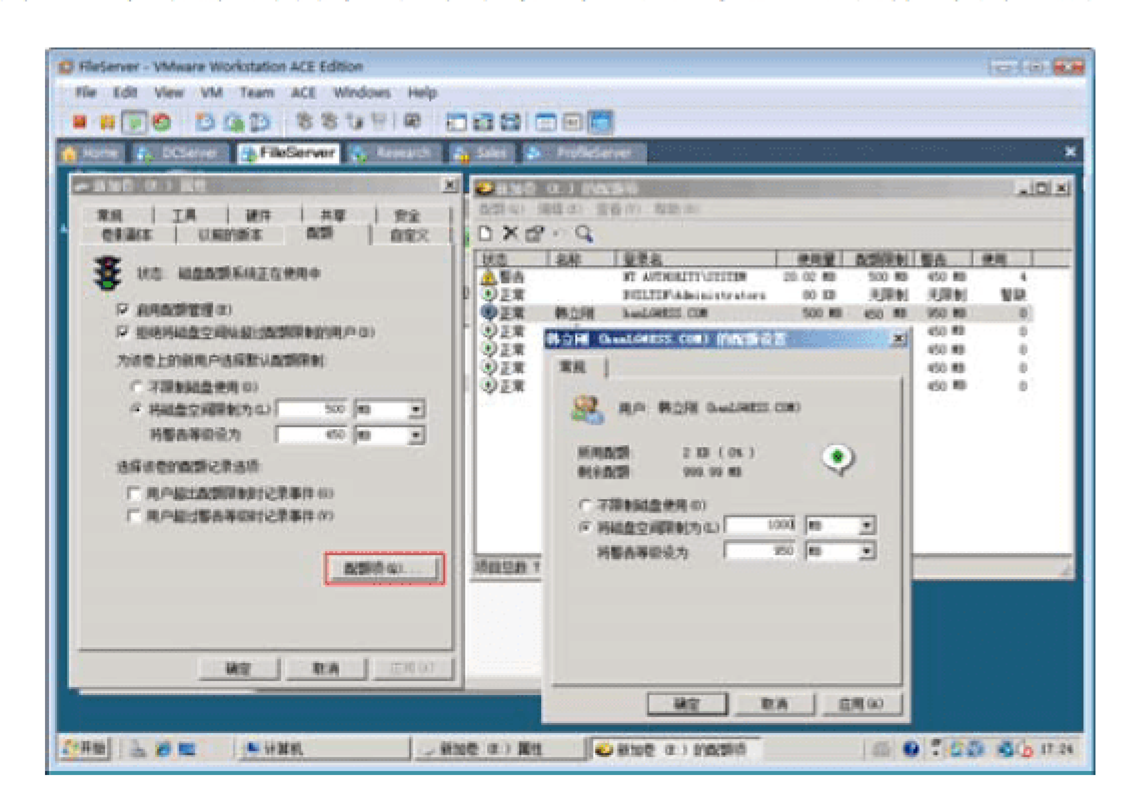


图 6-109 为特定用户指定特定大小的配额

6.7 卷影副本

共享文件夹的卷影副本提供位于共享资源(如文件服务器)上的实时文件副本。通过使用共享文件夹的卷影副本，用户可以查看在过去某个时刻存在的共享文件和文件夹。访问文件的以前版本或卷影副本非常有用，原因如下。

- 恢复意外删除的文件。如果你意外删除了某个文件，则可以打开前一版本，然后将其复制到安全的位置。
- 恢复意外覆盖的文件。如果你意外覆盖了某个文件，则可以恢复该文件的前一版本。
- 在处理文件的同时对文件版本进行比较。当你希望检查一个文件的两个版本之间发生的更改时，可以使用以前的版本。

注意事项

- 当你恢复文件时，文件权限不会更改。权限在恢复前后没有变化。当你恢复一个意外删除的文件

时，文件权限将被设为该目录的默认权限。

- 创建卷影副本不能替代创建常规备份。
- 当存储区域达到限制值之后，系统将删除最旧的卷影副本，从而留出空间以便创建更多卷影副本。删除卷影副本之后，将无法检索该副本。
- 可以调整存储位置、空间分配和计划以适合用户需要。在“本地磁盘属性”页面的“卷影副本”选项卡中，单击“设置”按钮。
- 每个卷上最多可以存储 64 个卷影副本。达到该限制值之后，将删除最旧的卷影副本，因此将无法检索该副本。
- 卷影副本是只读的。不能编辑卷影副本的内容。
- 只能针对每个卷启用共享文件夹的卷影副本，也就是说，不能在卷上选择要进行复制或不进行复制的特定共享文件夹和文件。

6.7.1 启用和配置“共享文件夹的卷影副本”

只能以卷为单位启用共享文件夹的卷影副本，也就是说，不能单独指定要复制或不复制卷上的特定共享文件夹和文件。此外，不应使用此功能来创建操作系统正确运行所需的文件卷影副本。

示例：启用和配置共享文件夹的卷影副本。

① 以管理员的账户登录 FileServer。

② 在 E 卷上创建“研发图纸”，共享，设置共享权限：Everyone 为参与者。

③ 依次选择“开始”→“管理工具”命令，然后单击“计算机管理”选项。

④ 如图 6-110 所示，在控制台树中，右击“共享文件夹”。在弹出的快捷菜单中选择“所有任务”→“配置卷影副本”命令。

⑤ 如图 6-111 所示，在出现的“卷影副本”对话框中，选择 E 卷，单击“设置”按钮。

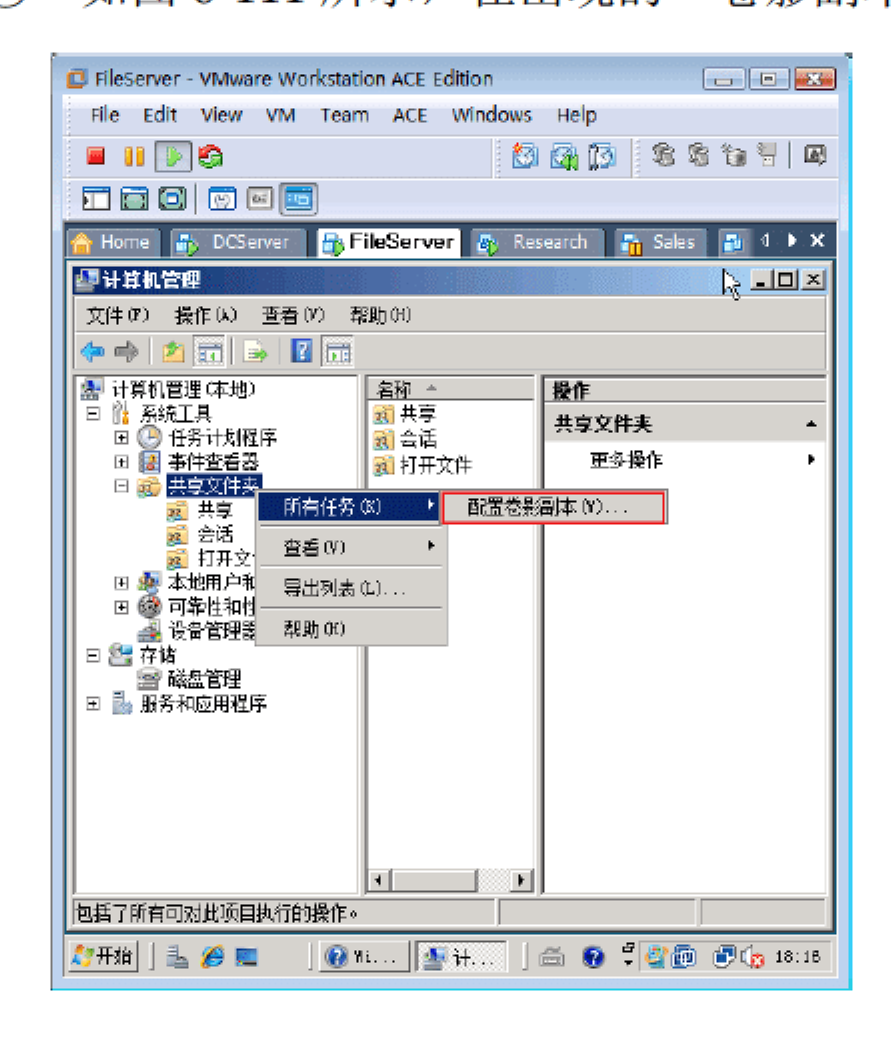




图 6-110 配置卷影副本

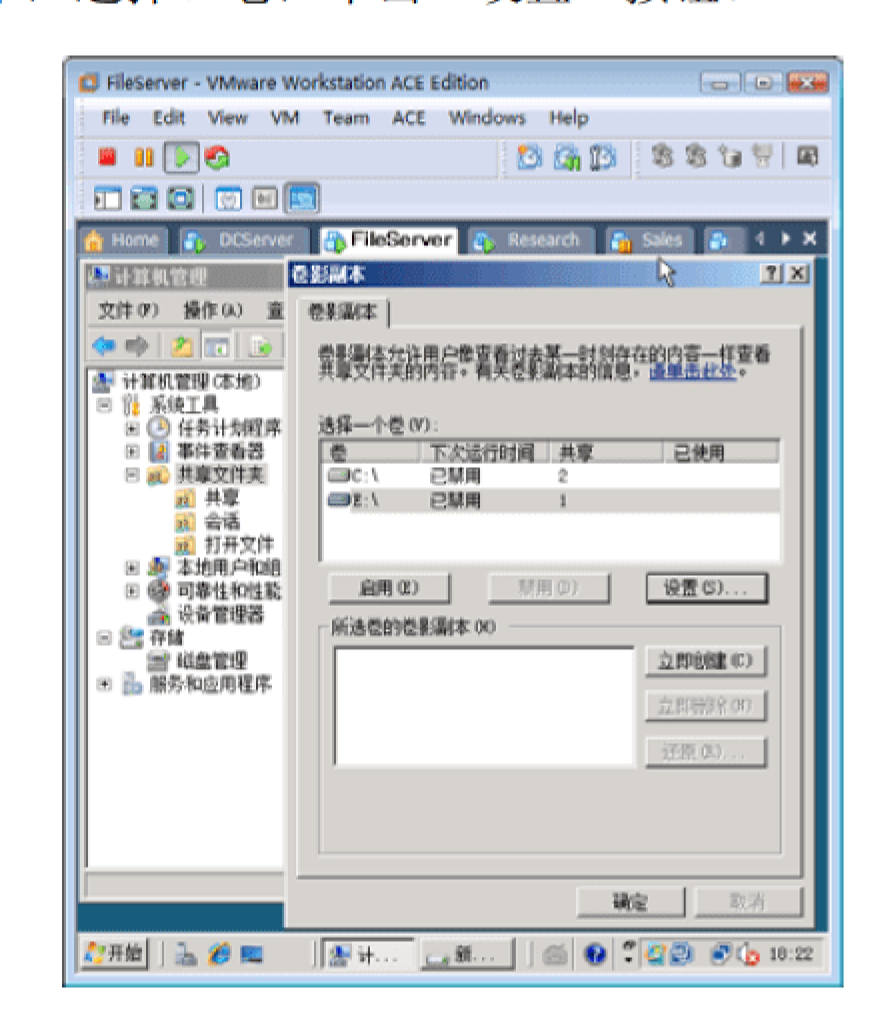


图 6-111 设置卷影副本

⑥ 如图 6-112 所示，在出现的“设置”对话框中，指定卷影副本存储位置以及大小。

⑦ 单击“计划”按钮，可以新建或修改创建卷影副本的计划，如图 6-113 所示。

注意：卷影副本会根据日程安排定时创建，现在做测试，可以通过单击“立即创建”按钮立刻产生副本。

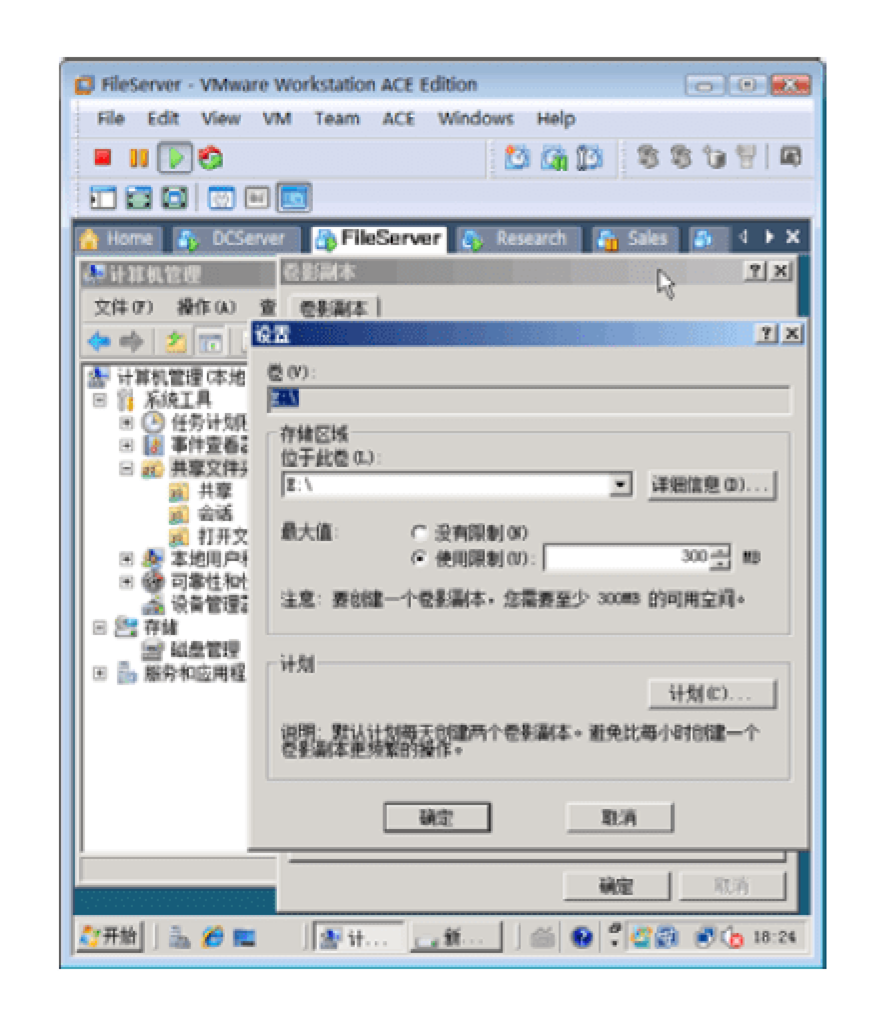


图 6-112　指定卷影副本的存储位置和大小

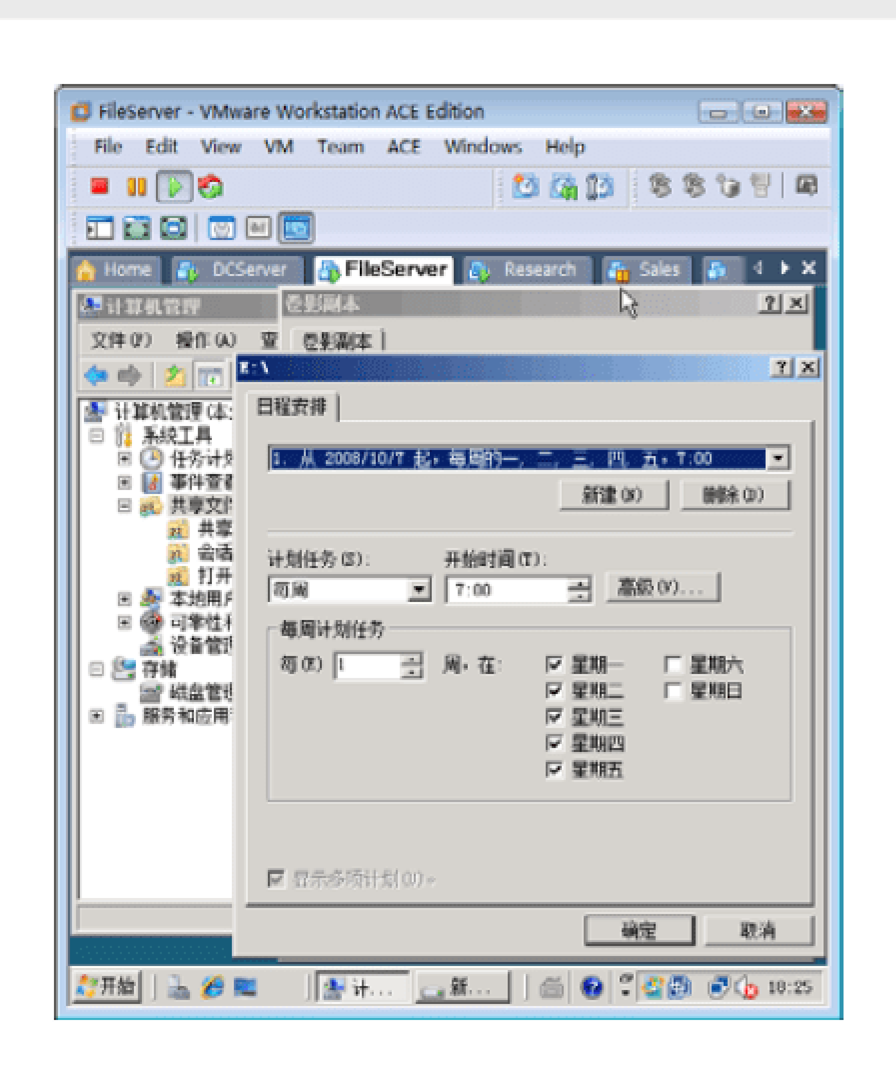


图 6-113　设置创建卷影副本的计划

⑧　单击“确定”按钮，然后单击“启用”按钮。

⑨　如图 6-114 所示，在 E 盘上“研发图纸”文件夹中创建 test.bmp 文件并保存。

⑩　如图 6-115 所示，右击 E 盘，在弹出的快捷菜单中选择“属性”命令，在打开的“新加卷属性”对话框中，切换到“卷影副本”选项卡，单击“立即创建”按钮。

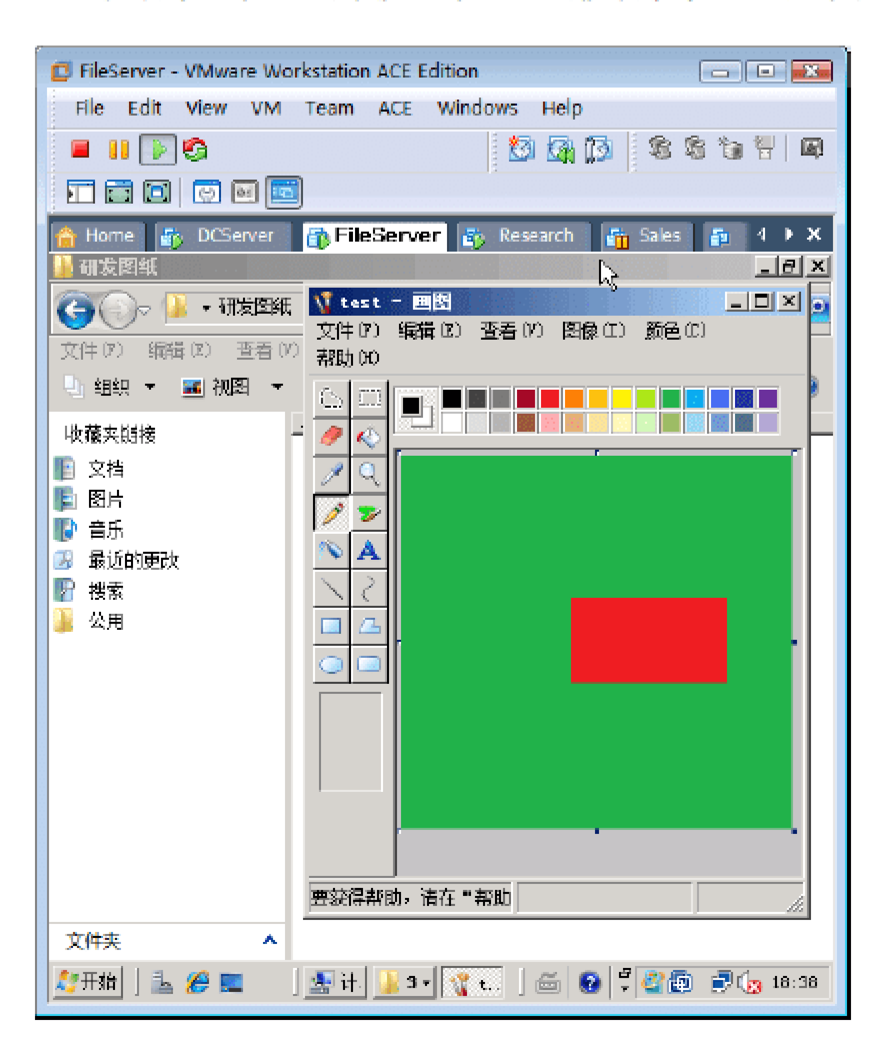


图 6-114　创建一个画图文件并保存

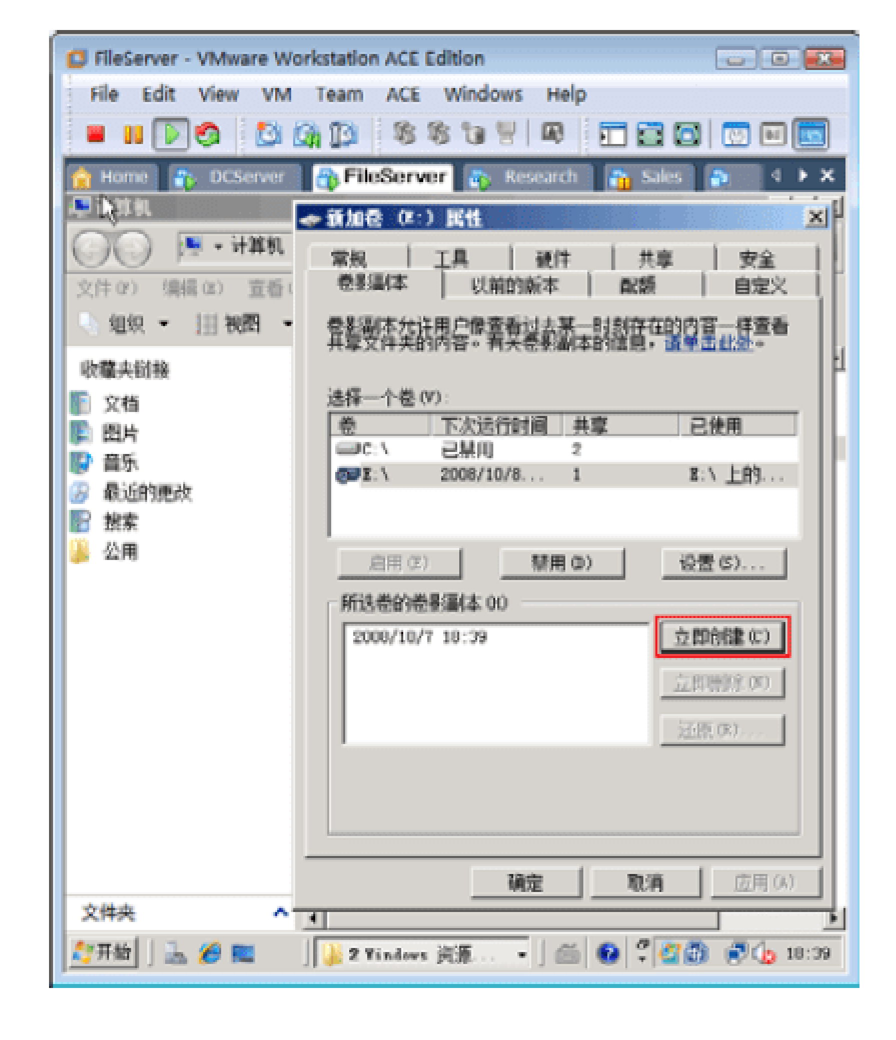


图 6-115　立即创建卷影副本

6.7.2　在本地找到以前版本的文件或文件夹

现在对 test.bmp 进行编辑并保存，然后还原到以前的状态。

演示：还原以前版本的文件或文件夹。

① 打开 test.bmp 文件，如图 6-116 所示，编辑并保存。

② 如图 6-117 所示，右击 E 盘，在弹出的快捷菜单中选择“属性”命令，在打开的对话框中，切换到“以前的版本”选项卡。可以看到刚刚创建的版本，单击“打开”按钮。

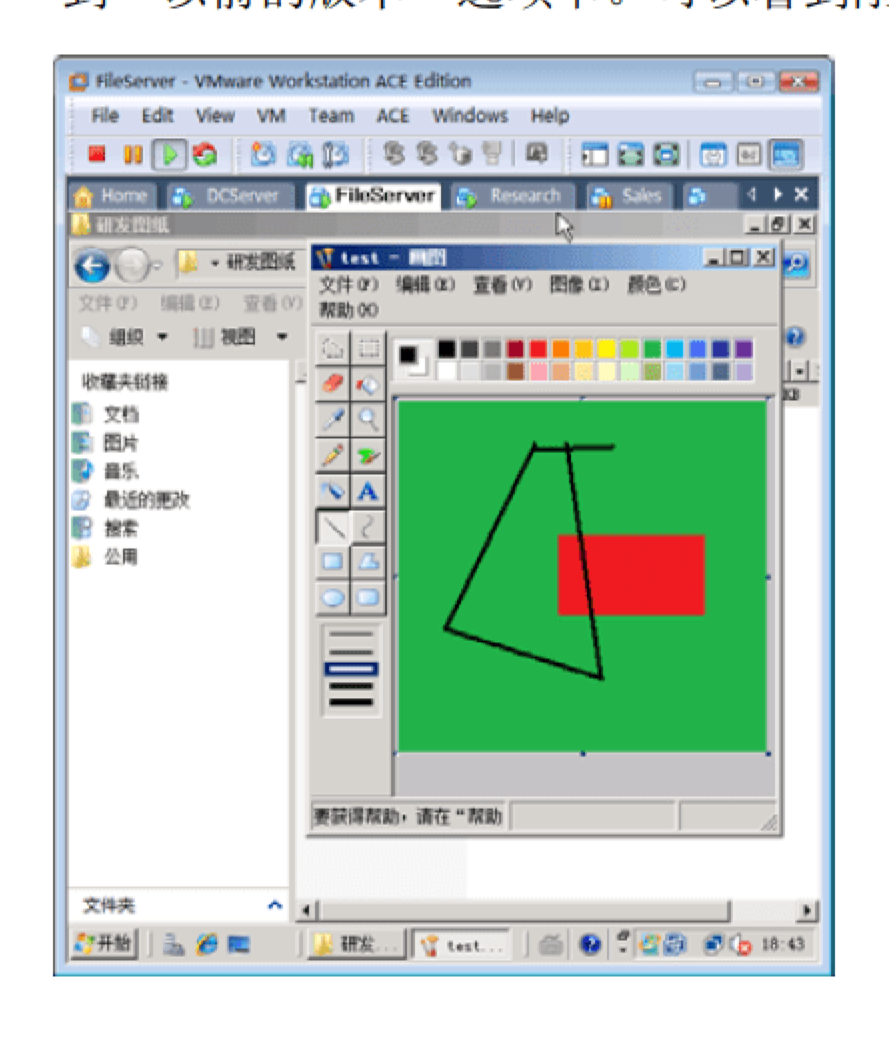




图 6-116 编辑并保存画图

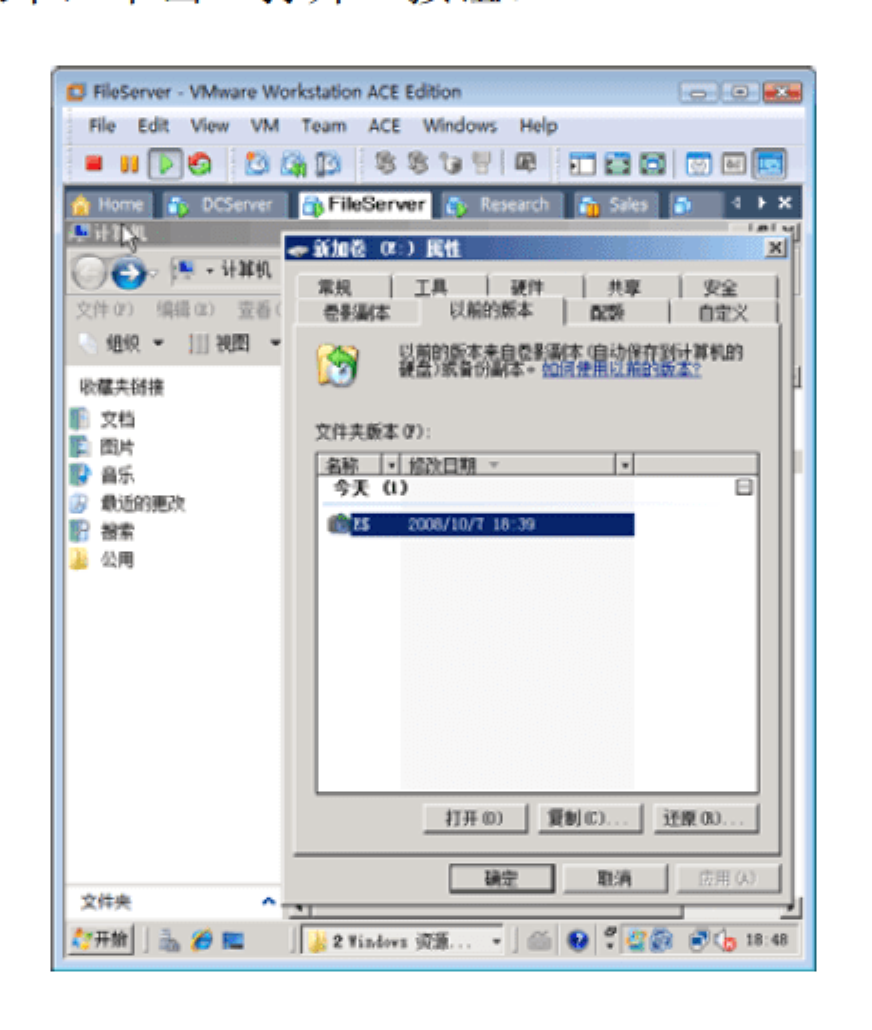


图 6-117 查看卷的以前版本

③ 如图 6-118 所示，双击 test.bmp 可以看到以前的版本。你可以复制到其他地方。

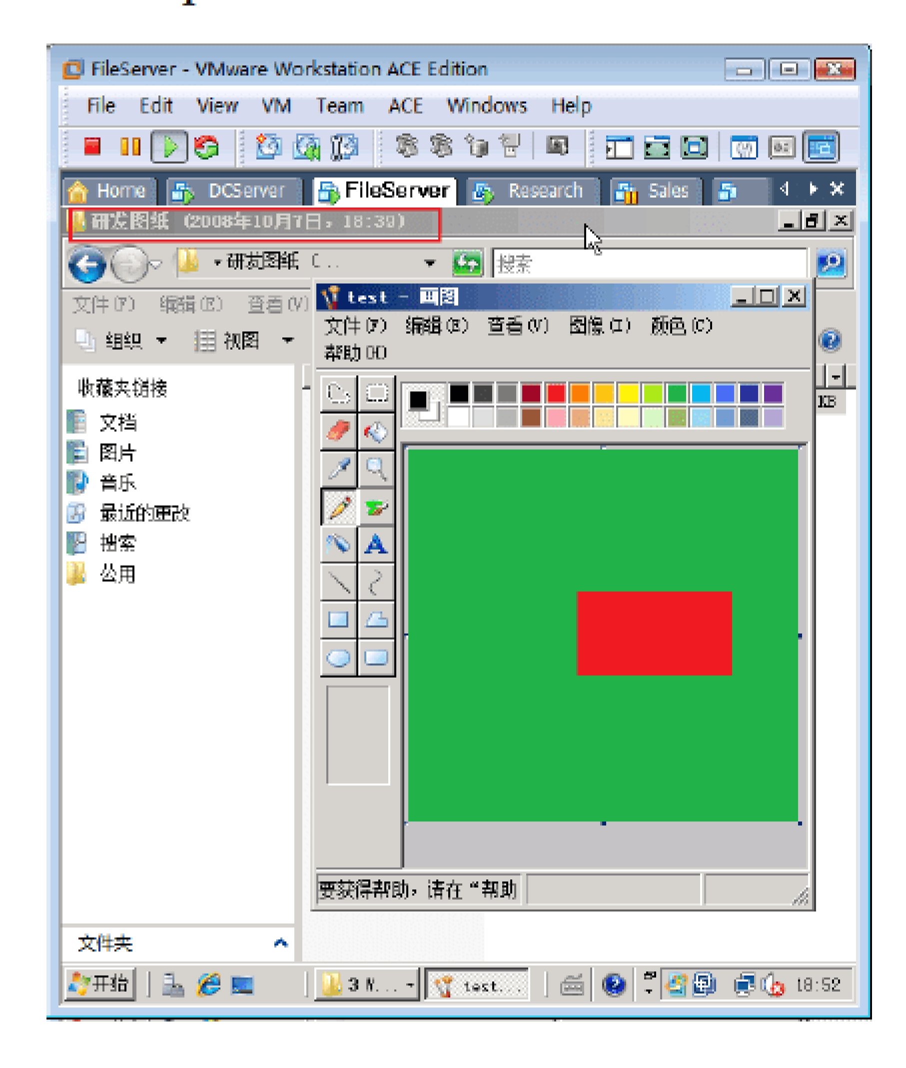


图 6-118 以前的版本

6.7.3 从共享文件夹中恢复数据

在 Research 计算机访问 FileServer 计算机上的共享文件“研发图纸”，并能够还原到以前的版本。删除文件 test.bmp，再还原删除的文件。

示例：从共享文件夹中恢复数据。

① 以域管理员的身份登录到 Research 计算机。

② 选择“开始”→“运行”命令，如图 6-119 所示，输入\\fileServer，单击“确定”按钮，打开共享的“研发图纸”文件夹。右击 test.bmp，在弹出的快捷菜单中选择“属性”命令，在属性对话框的“以前的版本”选项卡中，可以看到以前的版本。你可以还原、复制或打开该文件。

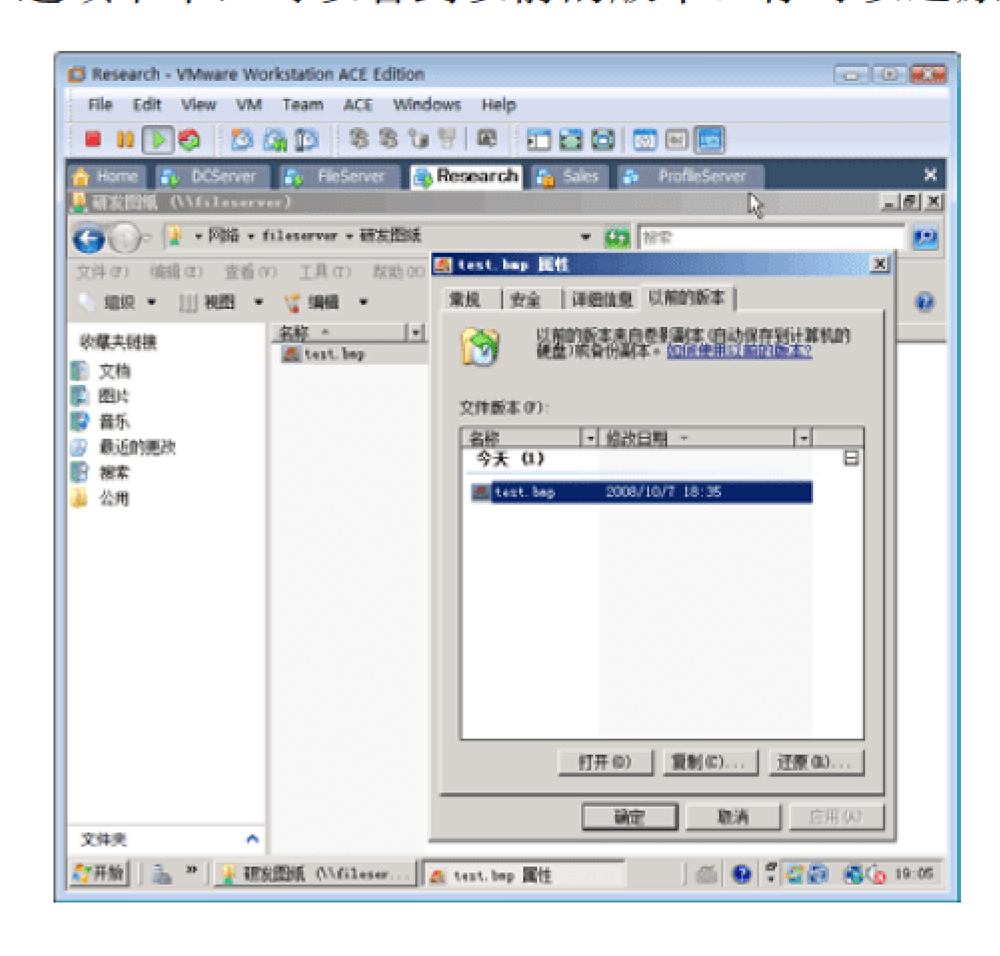


图 6-119　查看文件的以前版本

③ 删除 test.bmp 文件。

④ 如图 6-120 所示，右击“研发图纸”文件夹，在弹出的快捷菜单中选择“还原以前的版本”命令。在打开的“研发图纸属性”对话框中选中上一时间创建的副本，单击“打开”按钮。

⑤ 如图 6-121 所示，能够找到以前版本的 test.bmp 文件。

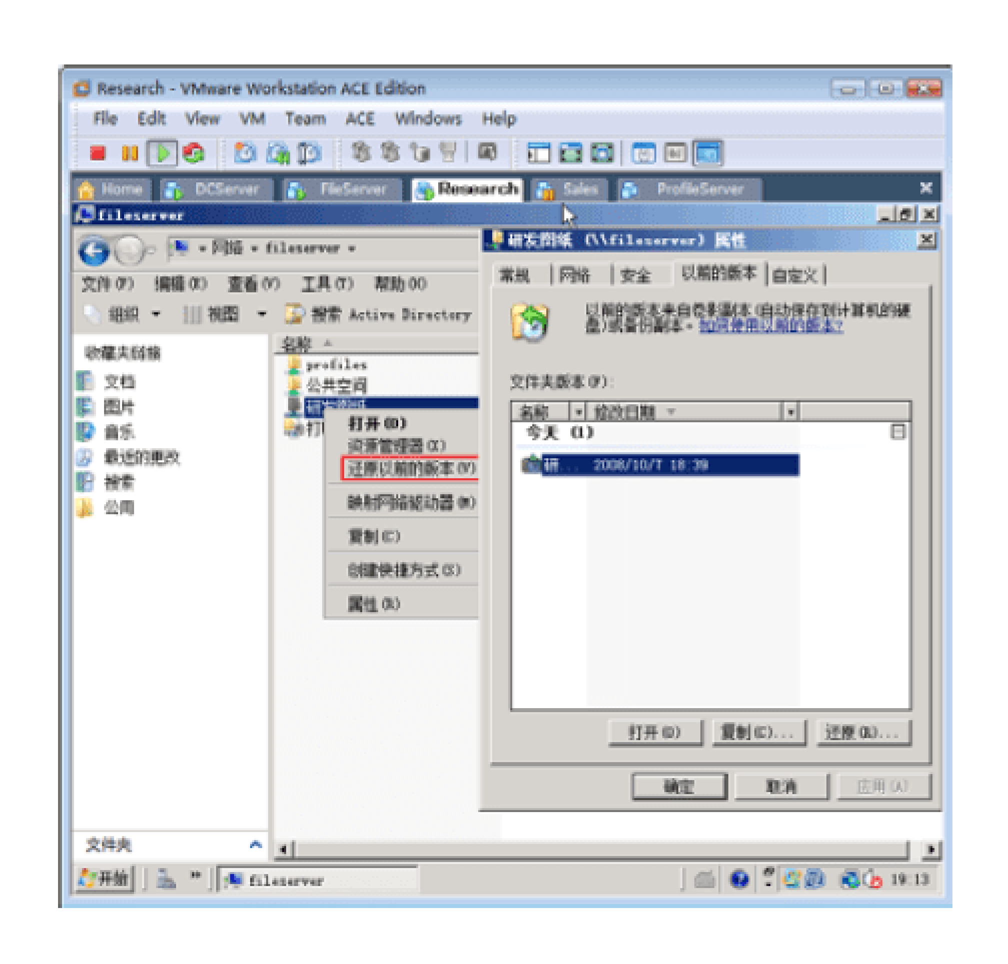


图 6-120　查看共享文件夹的以前版本

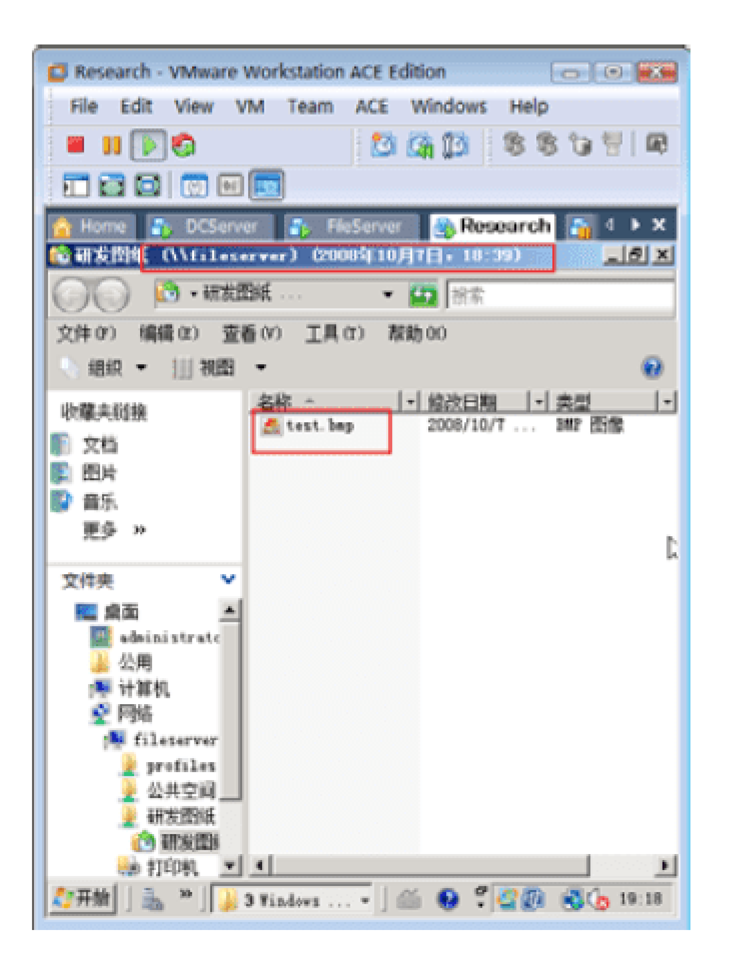


图 6-121　可以看到删除的文件

6.7.4　共享文件夹的卷影副本的最佳操作

共享文件夹的卷影副本的最佳操作如下。

- 在另一个磁盘上选择一个单独的卷作为卷影副本的存储区域。
- 在未进行卷影复制的磁盘上选择一个存储区域。如果使用另一个磁盘上单独的卷，将不会发生高 I/O 负载而导致卷影副本被删除，而且会大大提高性能。对于使用率高的服务器，这是推荐的配置。
- 考虑在启用共享文件夹的卷影副本并设置计划选项之前客户端使用共享资源的方式。
- 调整卷影副本计划以适合客户端的工作模式。
- 不要在使用装入点的卷上启用卷影副本。
- 当获取卷影副本时，安装的驱动器将不包括在内。仅在没有装入点的卷上启用卷影副本，或者在不希望对安装卷上的共享资源进行卷影复制时启用卷影副本。
- 对文件服务器执行常规备份。
- 共享文件夹的卷影副本不能替代执行常规备份。将备份实用程序和共享文件夹的卷影副本结合使用，作为最佳恢复准备。
- 不要将副本计划为每小时发生多次。
- 创建卷影副本的默认计划是周一到周五的早上 7:00 和中午。如果决定要更频繁地获取副本，应确认已分配了足够的存储空间，以及复制频率不会导致服务器性能降低。另外，还有一个上限，即每个卷最多可以存储 64 个副本，达到这个限制之后将删除最旧的副本。如果获取卷影副本太过频繁，可能会很快达到该限制值，时间较早的副本也会很快丢失。
- 在删除进行卷影复制的卷之前，要先删除用于创建卷影副本的计划任务。
- 如果在没有删除卷影副本任务的情况下删除卷，计划任务就会失败，事件日志中就会写入一个事件 ID 为 7001 的错误。在删除卷之前先删除任务，可避免事件日志中写入这些错误。
- 在格式化将要启用共享文件夹的卷影副本的源卷时，使用 16KB 或更大的分配单元。
- 如果计划对启用共享文件夹的卷影副本的源卷进行磁盘碎片整理，建议在初次对源卷进行格式化时，将群集分配单元的大小设为 16 KB 或更大。如果不这样做，由磁盘碎片整理导致的更改数量可能会导致以前版本的文件被删除。

第 7 章　搭建文件服务器

通过配置分布式文件系统(DFS)，将分散的网络资源逻辑地整合到一台计算机，可以简化访问者的访问，同时通过配置复制也能实现对分支办公室的支持，实现数据在多个服务器上的同步。

通过配置，用户可以脱机使用文件服务器上的文件夹。

安装文件服务器角色后能够限制文件夹大小以及文件夹中存放文件的类型。

关键词

- 理解哪些身份能够共享资源
- 学会设置共享权限
- 能够多次共享
- 学会隐含共享资源
- 能够访问隐含共享的文件夹
- 能够访问默认共享
- 学会配置分布式文件系统(DFS)
- 设计分布式文件系统
- 脱机使用文件夹
- 限制文件夹的大小
- 限制文件夹存放的文件类型

7.1 文件共享基础

可以通过几种不同的方式共享文件和文件夹。Windows 中最常用的共享文件方式是直接通过计算机共享。

7.1.1 Windows Server 2008 共享方式

Windows 提供了共享文件夹的两种方法：通过计算机上的任何文件夹或公用文件夹共享文件。

使用哪种方法取决于保存的共享文件夹的位置，要与哪些用户共享，以及对共享文件的控制程度。这两种方法均可实现与使用本地计算机或同一网络中其他计算机的用户共享文件或文件夹。

1. 通过计算机上的任何文件夹共享文件

通过这种共享方法，可以决定哪些人可以更改共享文件，以及可以做什么类型的更改(如果有)。可以通过设置共享权限进行操作。可以将共享权限授予同一网络中的单个用户或一组用户。例如，可以允许某些人只能查看共享文件，而允许其他人既可查看又能更改这些文件。采用这种方式共享用户将只能看到与其共享的那些文件夹。

当使用同一网络中的其他计算机时，还可以使用此共享方法来访问共享文件，因为用户可以通过其他计算机查看与其他人共享的任何文件。

2. 通过计算机上的公用文件夹共享文件

通过这种共享方法，可将文件复制或移动到公用文件夹中，并通过该位置共享文件。如果打开公用文件夹的文件共享，本地计算机上具有用户账户和密码的任何人，以及网络中的所有人，都可以看到公用文件夹和子文件夹中的所有文件。使用这种共享方式不能限制用户只能查看公用文件夹中的某些文件。但是，可以设置权限，以完全限制用户访问公用文件夹，或限制用户更改文件或创建新文件。

另外，还可以设置密码保护的共享。这使得只具有计算机的用户账户和密码的用户才具有对公用文件夹的网络访问权限。在默认情况下，将关闭对公用文件夹的网络访问，除非启用它。

3. 哪些用户能够共享文件夹

- Administrators 组的账号可以设置共享。
- Power user 组的账号也可以设置共享文件夹。
- 普通用户没有权限设置共享。

7.1.2 使用哪种共享方法

在决定通过任何文件夹共享文件或通过公用文件夹共享文件时，有几个因素需要考虑。

以下情况可考虑通过任何文件夹共享。

- 你倾向于直接从文件的保存位置(一般是 Documents、Pictures 或 Music 文件夹)共享文件夹，且希望避免将其保存到公用文件夹中。

- 你希望能够为网络中的单个用户而不是每个人设置共享权限，向某些人授予更多或更少访问权限(或无任何访问权限)。
- 你需要共享大量数字图片、音乐或其他大文件，而将这些文件复制到单独的共享文件夹很麻烦，并且不希望这些文件在计算机上的两个不同位置占用空间。
- 你经常创建新文件或更新文件进行共享，并认为将其复制到公用文件夹很麻烦。

以下情况可考虑通过公用文件夹共享。

- 你喜欢通过计算机的单个位置共享文件和文件夹带来的方便。
- 你希望只通过查看公用文件夹即可快速查看与其他人共享的所有文件。
- 你希望将共享的文件与自己的 Documents、Music 和 Pictures 文件夹分开。
- 你希望为网络上所有人设置共享权限，而不必为单个用户设置共享权限。

7.1.3　与共享相关的服务

如图 7-1 所示，如果取消选中本地连接“Microsoft 网络客户端”复选框，则该计算机不能访问其他服务器上的共享资源。

如果取消选中“Microsoft 网络的文件和打印机共享”复选框，则其他计算机不能从这块网卡访问该计算机的共享文件夹和打印机。

如图 7-2 所示，Proxy 服务器连接 Internet 和内网，同时还共享了一个文件夹供内网用户使用。若不想让 Internet 的用户访问 Proxy 共享文件夹，需要将“Internet 连接”取消选中“Microsoft 网络的文件和打印机共享”复选框，“内部连接”选项保留，那么内网的计算机就能通过“内部连接”访问 Proxy 服务器上的共享文件夹，而 Internet 上的用户不能通过“Internet 连接”访问该服务器上的共享文件夹，这样可以保证 Proxy 服务器的安全。

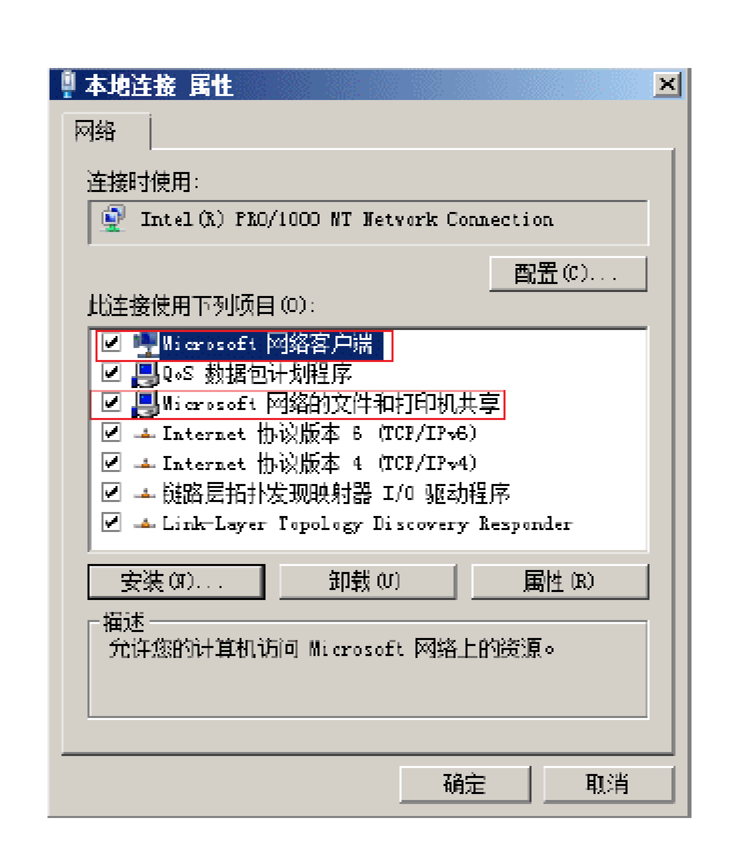



图 7-1　与共享有关的设置

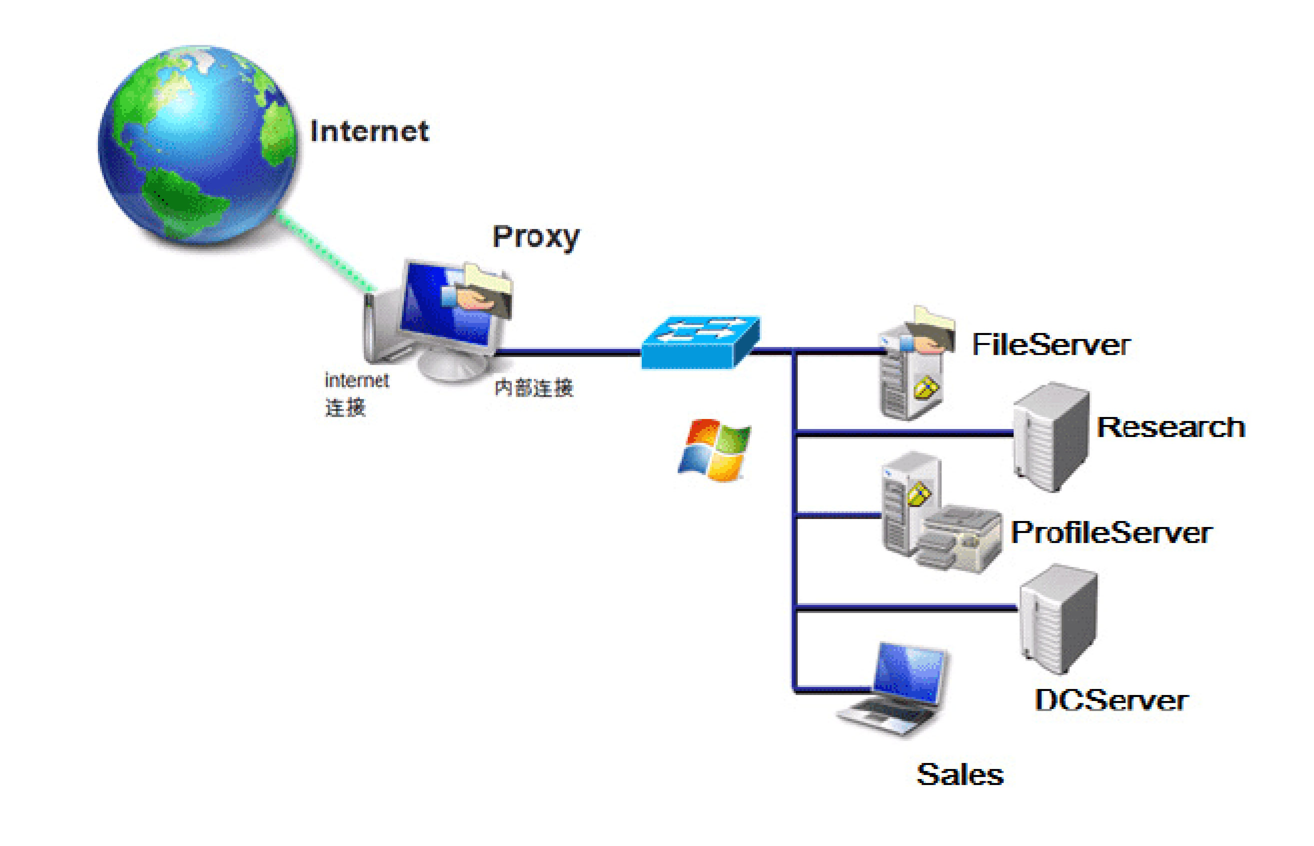


图 7-2　网络示意图

7.1.4　共享权限和 NTFS 权限

1. 共享权限

共享权限有三种：读者、参与者和所有者。



注意： 共享权限只对从网络访问该文件夹的用户起作用，而对于本机登录的用户不起作用。

2. NTFS 权限

NTFS 权限是 NT 和 Windows 2000、Windows 2008 中的文件系统的权限，它支持本地安全性。换句话说，它在同一台计算机上以不同用户名登录，对硬盘上同一文件夹可以有不同的访问权限。



注意： NTFS 权限对从网络访问和本机登录的用户都起作用。

3. 共享权限和 NTFS 权限的联系和区别

共享权限是基于文件夹的，也就是说用户只能够在文件夹上而不可能在文件上设置共享权限；NTFS 权限是基于文件的，用户既可以在文件夹上设置也可以在文件上设置。

共享权限只有当用户通过网络访问共享文件夹时才起作用，如果用户是本地登录计算机则共享权限不起作用；NTFS 权限无论用户是通过网络还是本地登录使用文件都会起作用，只不过当用户通过网络访问文件时它会与共享权限联合起作用，规则是取最严格的权限设置。

共享权限与文件操作系统无关，只要设置共享就能够应用共享权限；NTFS 权限必须是 NTFS 文件系统，否则不起作用。

共享权限只有三种：读者、参与者和所有者；NTFS 权限有许多种，如读、写、执行、修改及完全控制等。我们可以进行非常细致的设置。

4. 共享权限和 NTFS 权限的特点

- 不管是共享的权限还是 NTFS 权限都有累加性。
- 不管是共享权限还是 NTFS 权限都遵循“拒绝”权限优先于其他权限。

当一个账户通过网络访问一个共享文件夹，而这个文件夹又在一个 NTFS 分区上，那么用户最终的权限是它对该文件夹的共享权限与 NTFS 权限中最为严格的权限。如：一个人要进一个院子，两道门都开才能进去，门就好像是权限。

7.1.5 默认共享

在 Windows 2000/XP/2003/2008 系统中，逻辑分区与 Windows 目录默认为共享，这是为管理员管理服务器的方便而设的。其权限不能更改。

7.2 实战 1：共享和访问共享文件夹

7.2.1 任务 1：共享文件夹

在 FileServer 服务器上创建“研发图纸”文件夹，设置共享权限为：“研发人员”为读者，归档员“张京灵”用户账户为参与者。

① 以域管理员身份登录 FileServer。
② 在 E 分区创建“研发图纸”文件夹。
③ 右击该文件夹，在弹出的快捷菜单中选择“属性”命令。
④ 如图 7-3 所示，在出现的“研发图纸 属性”对话框的“共享”选项卡中，单击“共享”按钮。

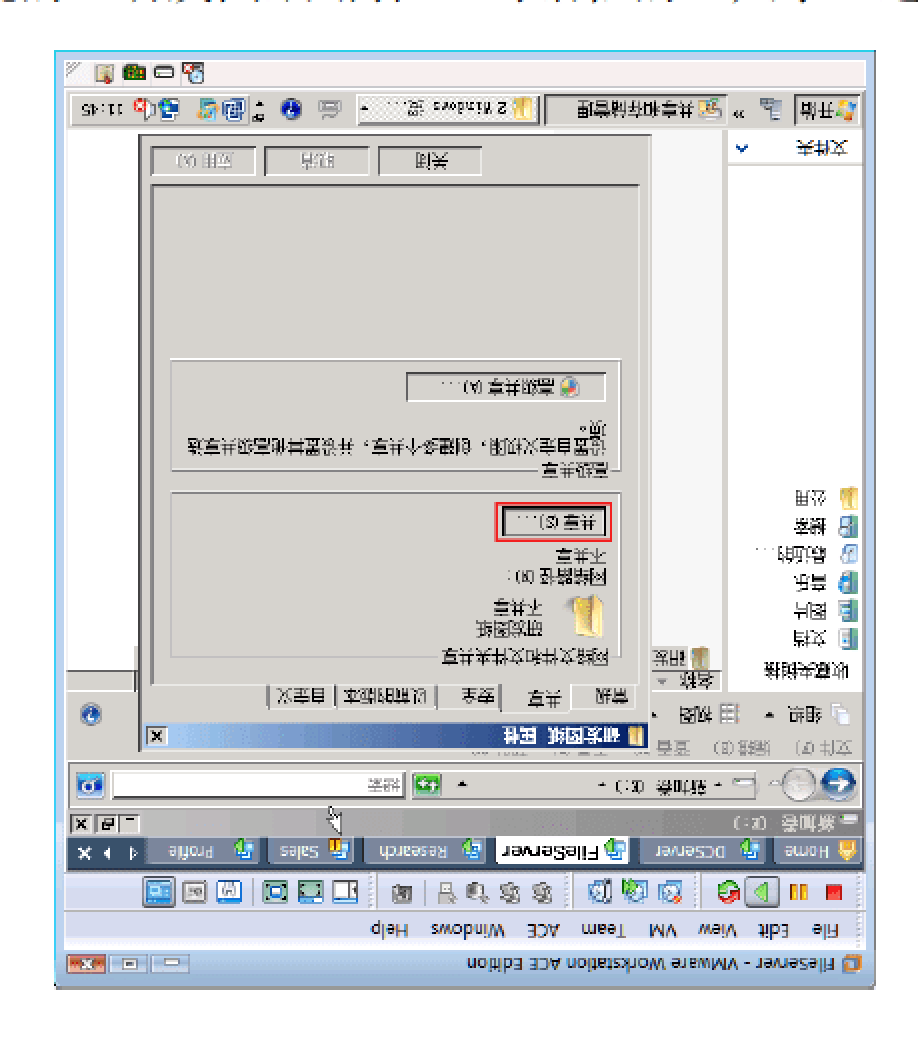
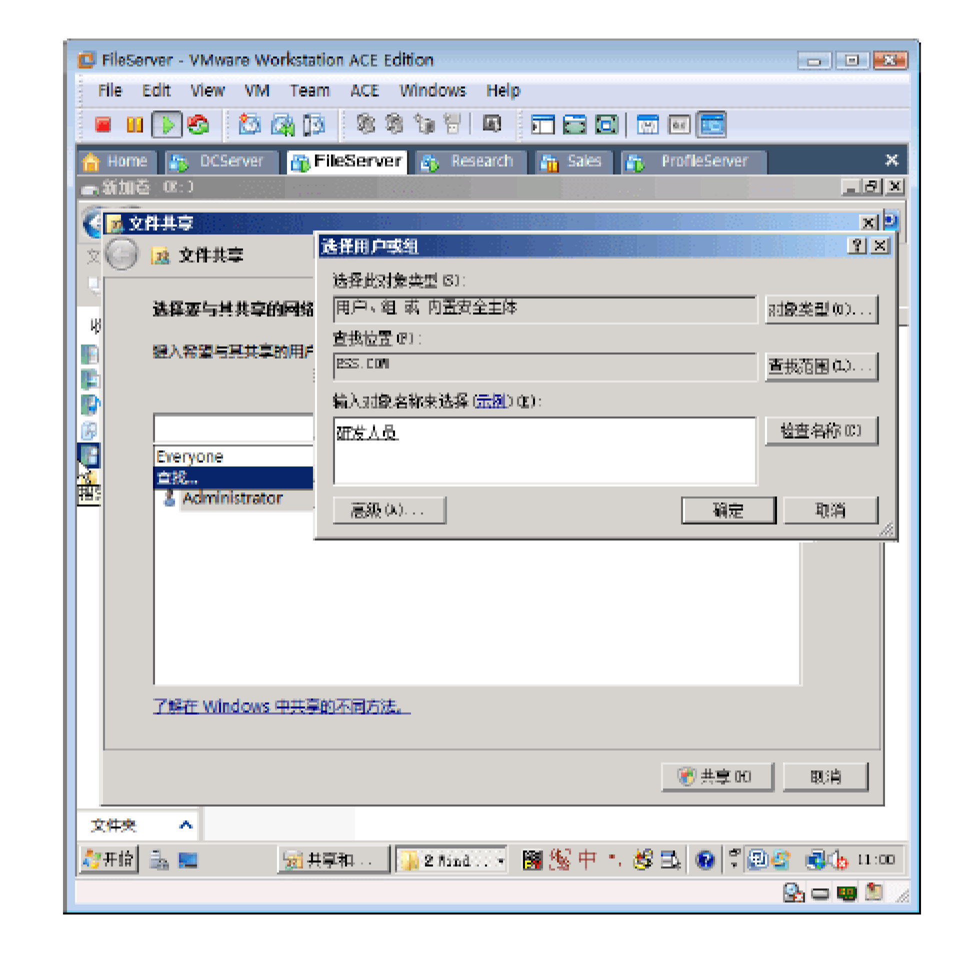


图 7-3　打开共享向导

⑤ 在弹出的“文件共享”对话框中，从下拉列表框中选择“查找”。
⑥ 如图 7-4 所示，在出现的“选择用户或组”对话框中，输入“研发人员”，单击“确定”按钮。
⑦ 再次单击下拉列表框右侧的下三角按钮，选择“查找”选项，输入“张京灵”，单击“确定”按钮。
⑧ 如图 7-5 所示，单击“张京灵”，将其权限级别设置为“参与者”。



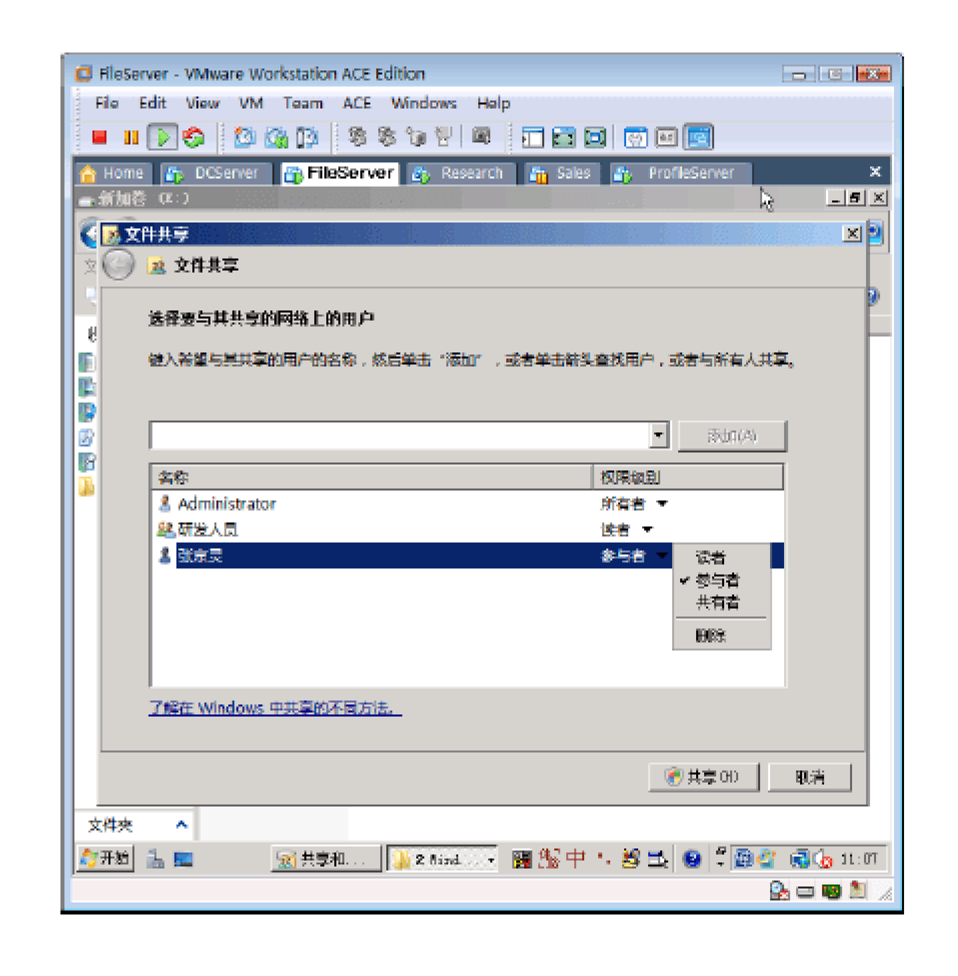




图 7-4　查找域中的组　　**图 7-5　设置共享权限**

⑨ 如图 7-6 和图 7-7 所示，在文件夹的“研发图纸 属性”对话框的“安全”选项卡中，可以看到张京灵和研发人员已经被授予能够实施共享权限必要的 NTFS 权限。

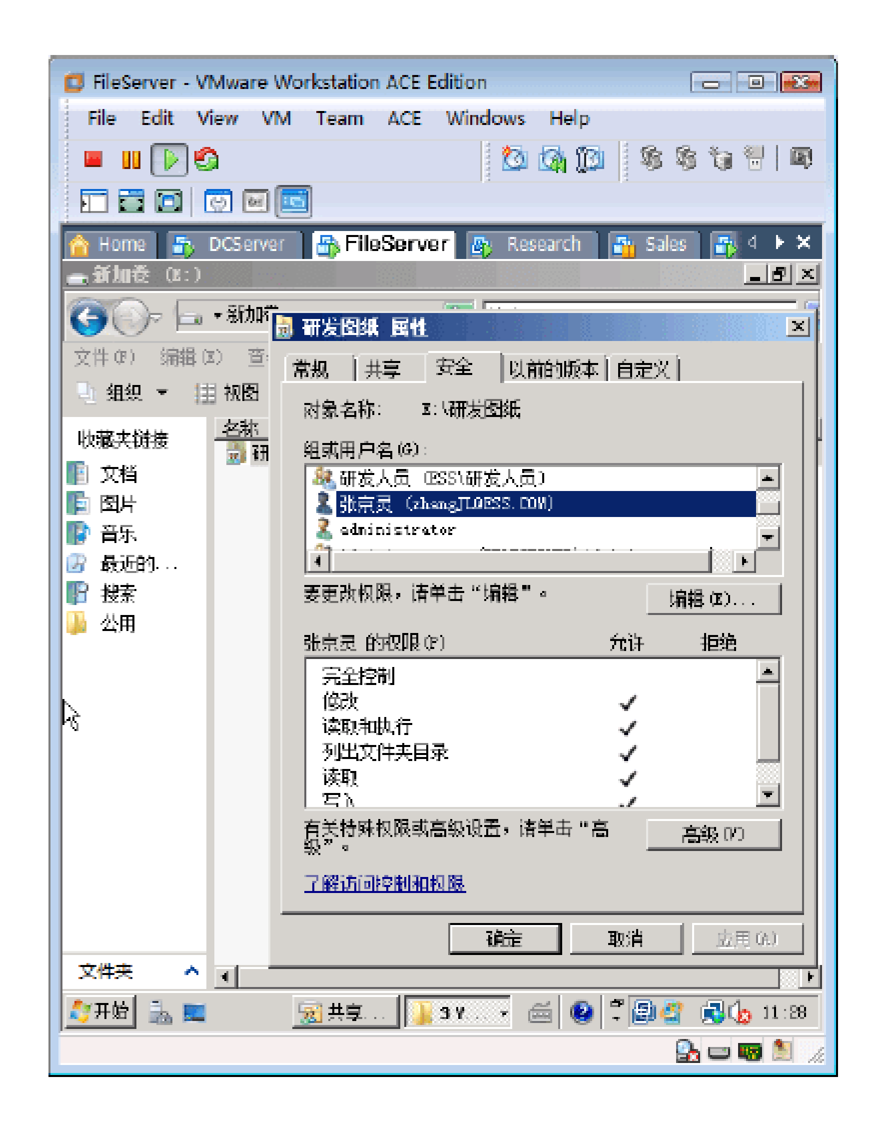


图 7-6 查看 NTFS 权限

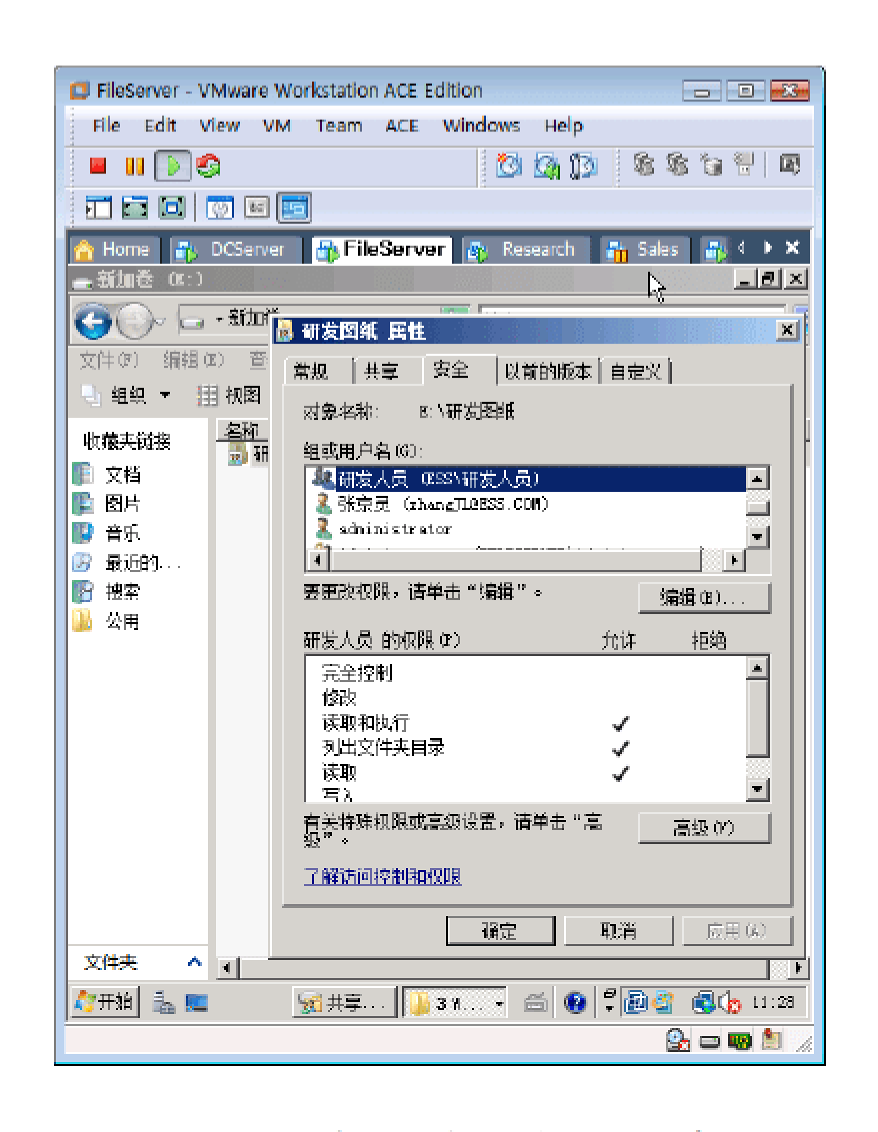


图 7-7 查看研发人员的 NTFS 权限

7.2.2 任务 2：停止共享

① 右击共享的“研发图纸”文件夹，在弹出的快捷菜单中选择“属性”命令。

② 如图 7-8 所示，在“研发图纸 属性”对话框的“共享”选项卡中，单击“共享”按钮。

③ 如图 7-9 所示，在出现的“文件共享”对话框中，选中“停止共享”单选按钮，单击“完成”按钮。

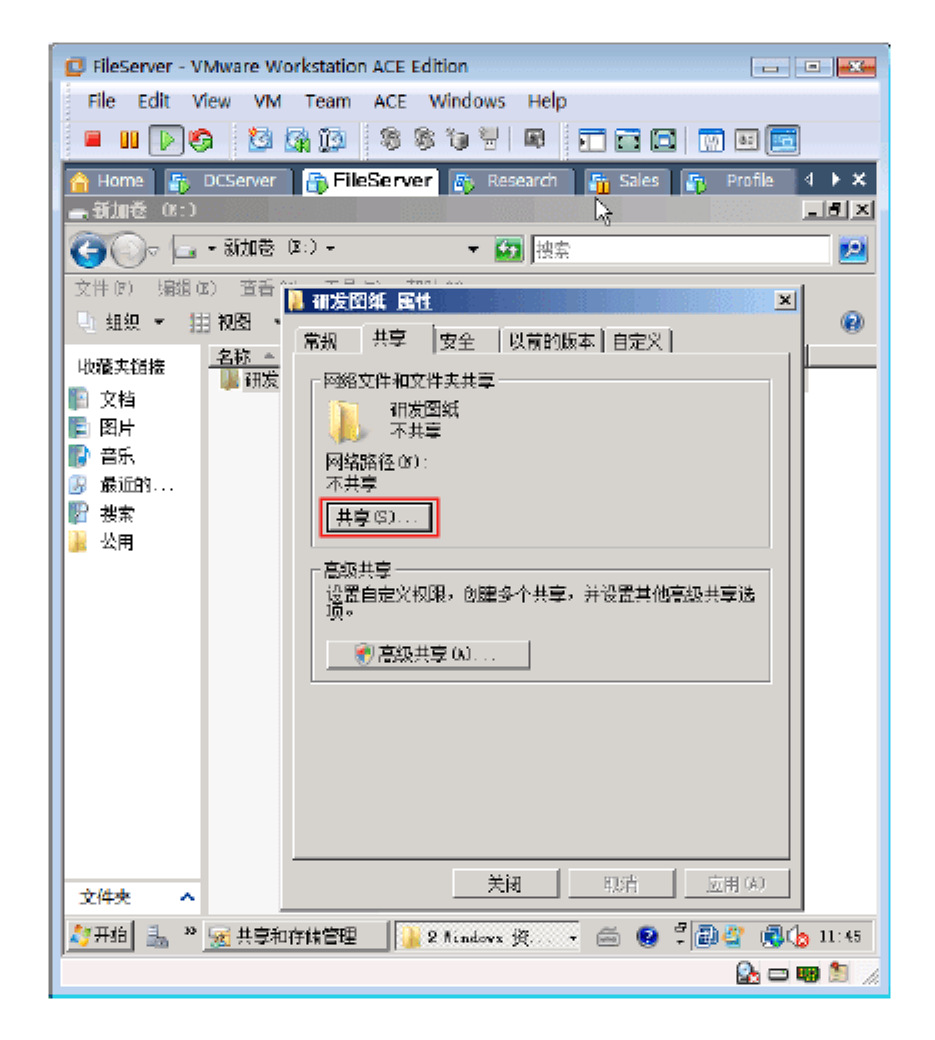


图 7-8 更改共享

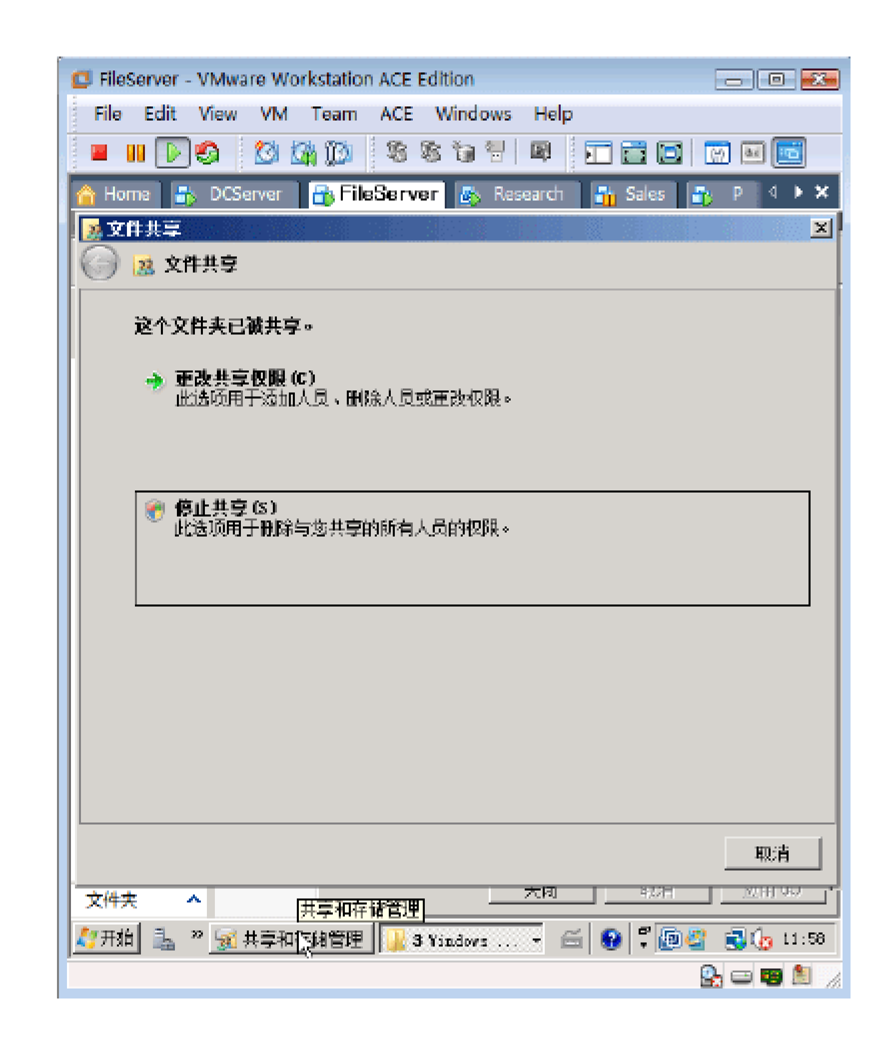


图 7-9 停止共享

④ 如图 7-10 所示，再次查看该文件夹的 NTFS 权限，可以发现已经共享时添加的“研发人员”和“张京灵”对该文件夹的授权已经取消。

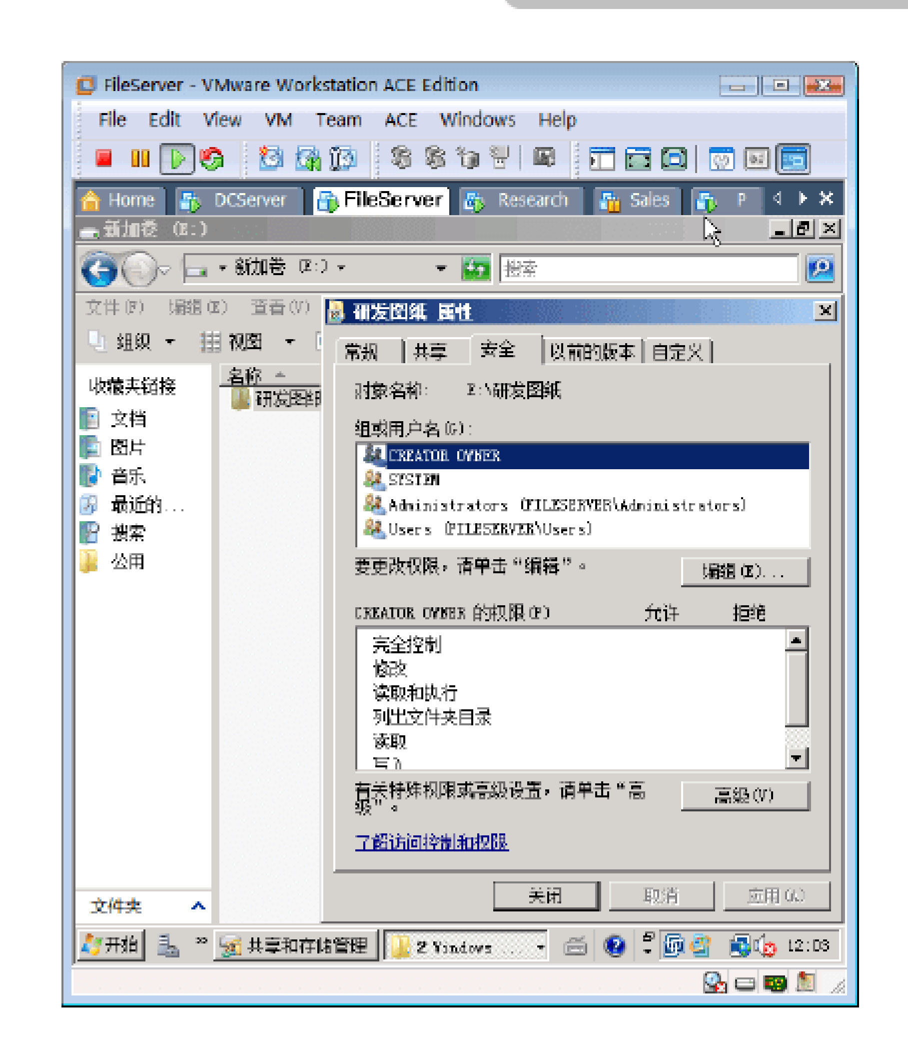


图 7-10　再次查看共享权限

7.2.3　任务 3：高级共享

使用高级共享的更多设置

① 如图 7-11 所示，在“研发图纸 属性”对话框的“共享”选项卡中，单击“高级共享”按钮。

② 如图 7-12 所示，在“高级共享”对话框中，选中“共享此文件夹”复选框，输入共享名“研发资料”，指定并发连接该共享文件夹的用户数量：100，单击“权限”按钮。

注意： 共享名在计算机上必须唯一，不能以相同的名称共享多个文件夹。共享名可以和文件夹名称不一样。

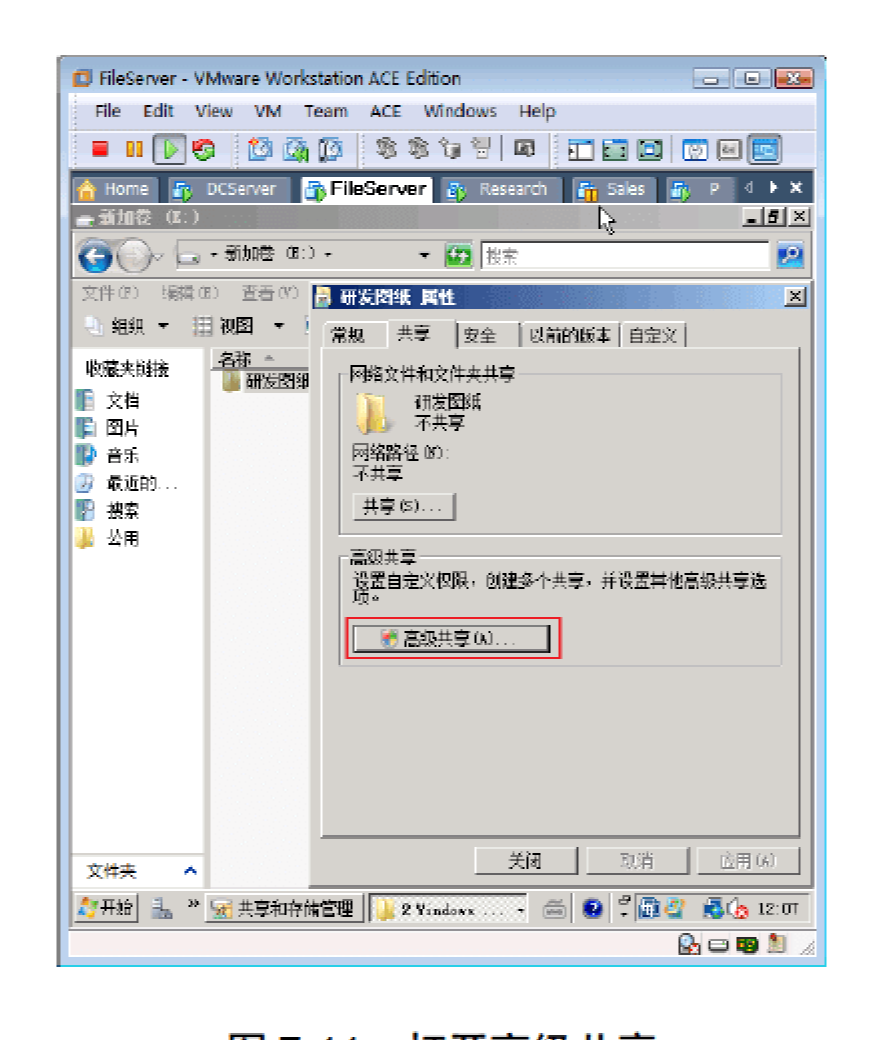


图 7-11　打开高级共享

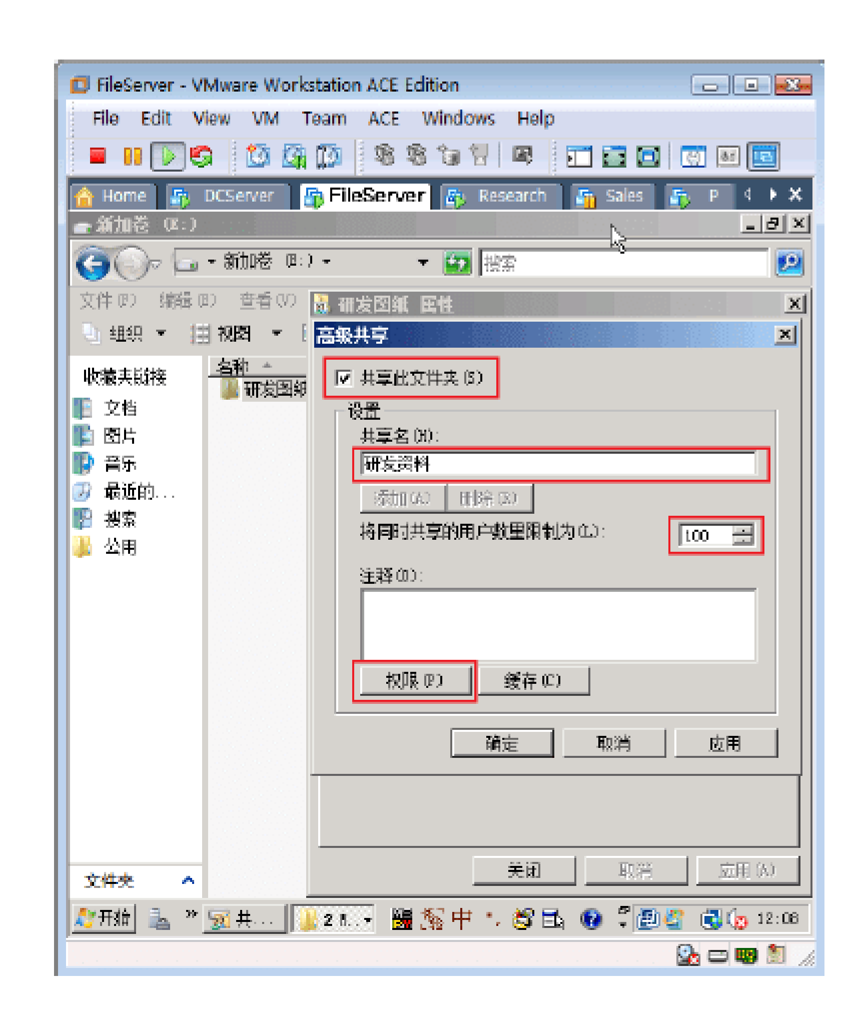


图 7-12　设置共享权限和并发连接数

③ 在出现的如图 7-13 所示的对话框中，删除 Everyone 用户的读取权限，添加“研发人员”，授予读取权限，添加“张京灵”，授予更改和读取权限，单击“确定”按钮，完成共享设置。添加域

管理员读取权限。

④ 打开研发资料属性的“安全”选项卡，发现使用高级共享后，NTFS 权限并没有改变，如图 7-14 所示。需要单独设置“张京灵”和“研发人员”的 NTFS 权限。

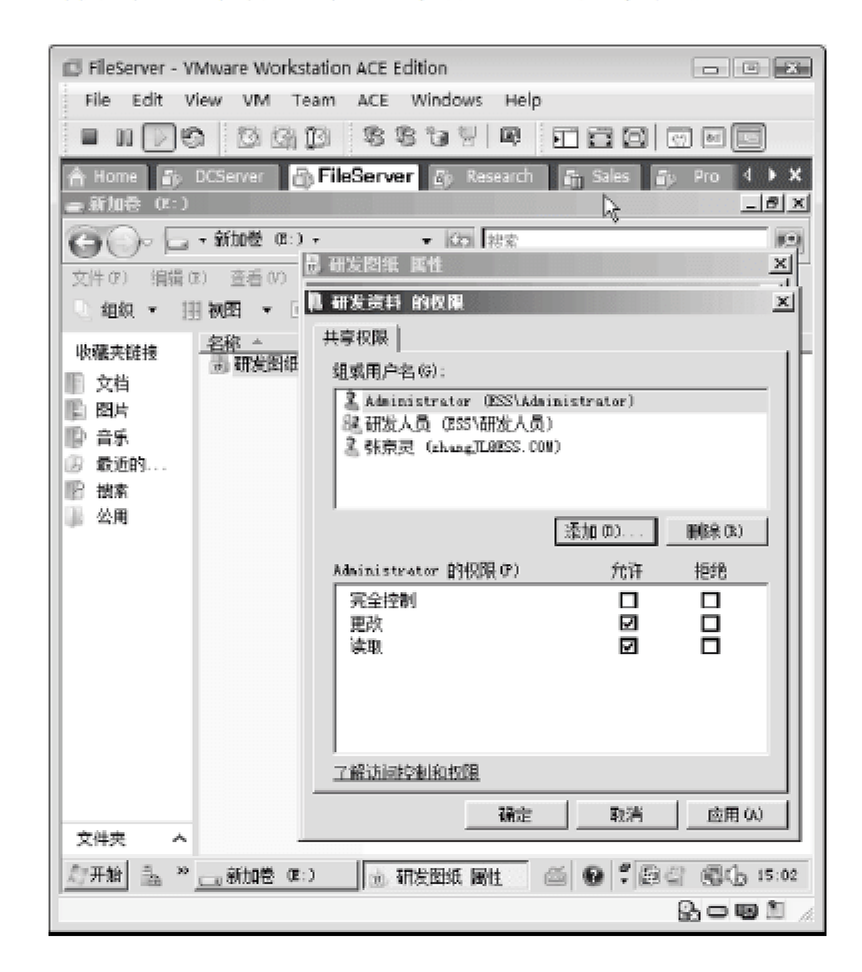


图 7-13　更改共享权限

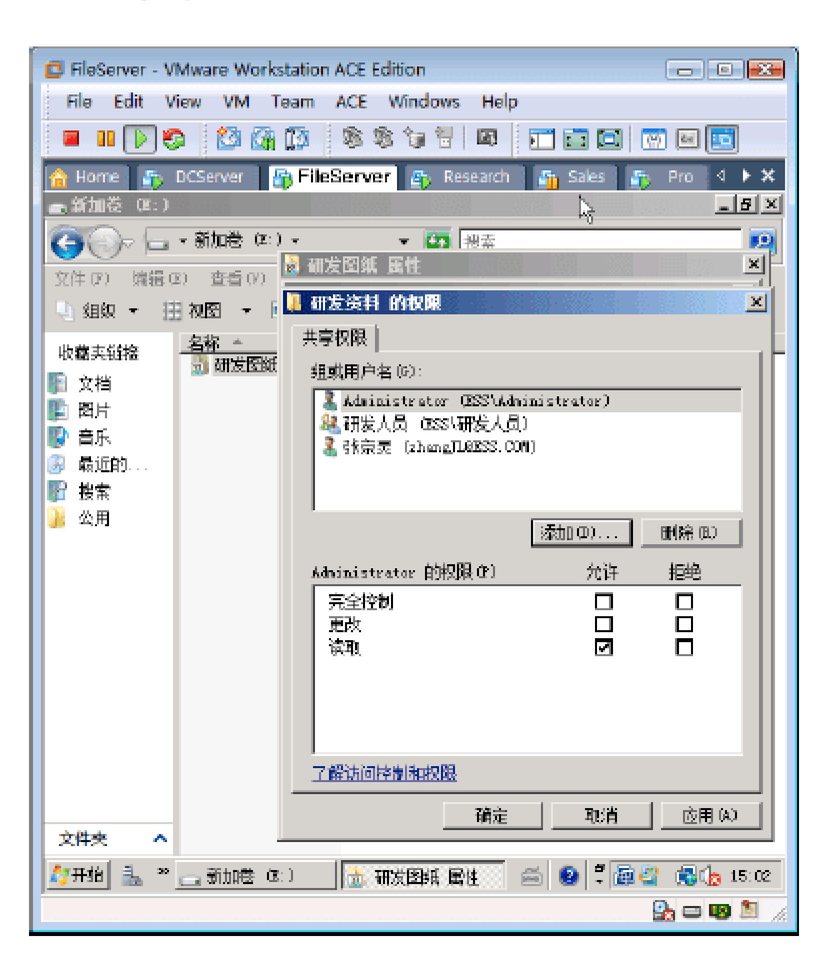


图 7-14　再次检查 NTFS 权限

7.2.4　任务 4：创建隐含共享的文件夹

一个文件夹可以使用多个共享名共享，设置不同的共享权限。如果你不想让共享的文件夹在网络上被看到，可以设置隐含共享。

隐含共享只需要在共享名后面添加“$”符号即可。

给共享的文件夹“研发图纸”添加一个隐含共享 YF$，设置管理员能够完全控制。

① 如图 7-15 所示，在“研发图纸 属性”对话框的“共享”选项卡中，单击“添加”按钮。

② 如图 7-16 所示，输入共享名 YF$，允许的用户数量为 1。

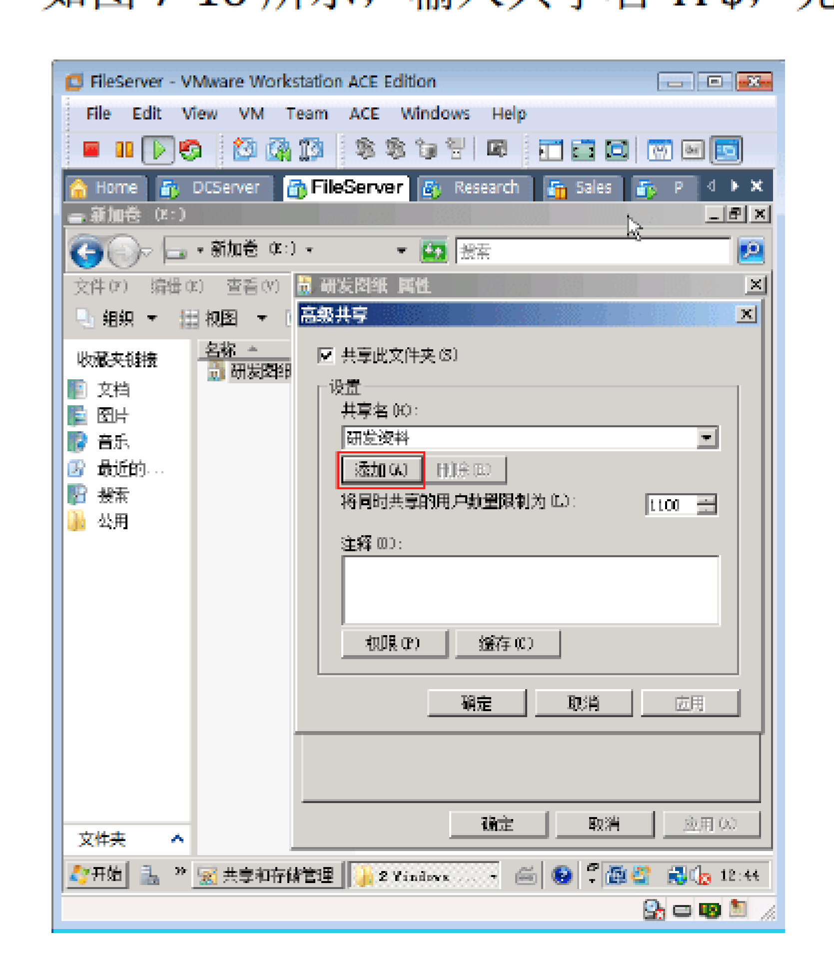


图 7-15　添加共享名

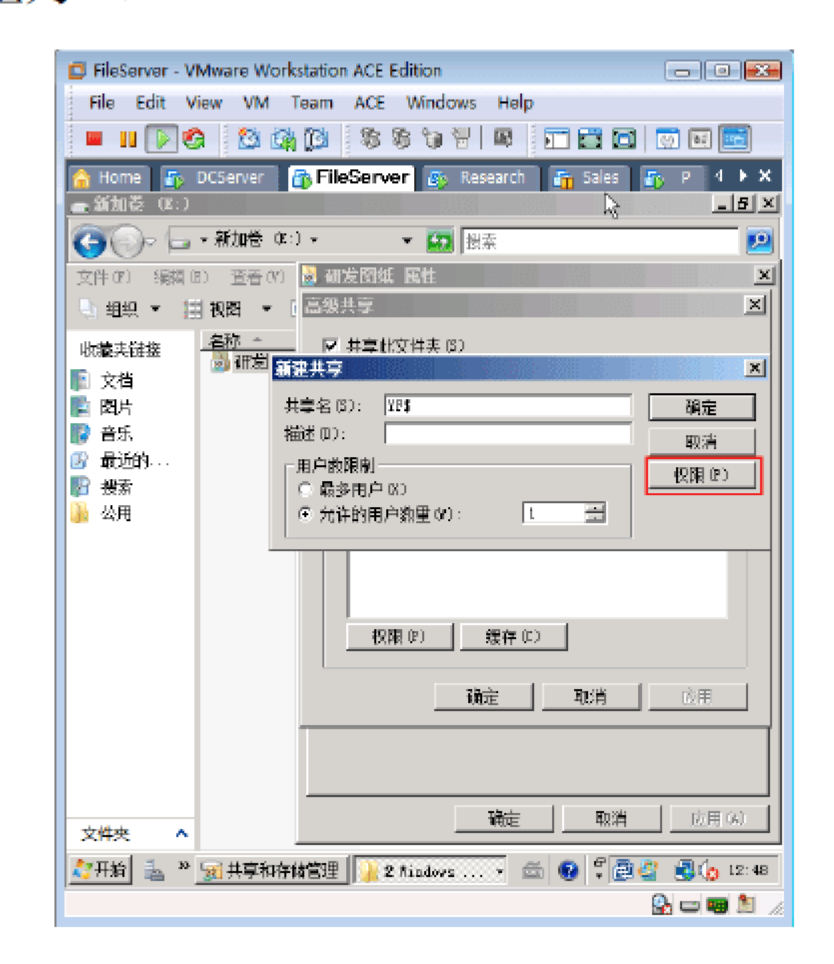


图 7-16　隐含共享

③　如图 7-17 所示，单击“权限”按钮，删除 Everyone 账户的权限。

④　如图 7-18 所示，添加域管理员能够完全控制。单击“确定”按钮。

⑤　添加完隐含共享后，单击“共享名”下拉列表框的下三角按钮，可以看到该文件夹的所有共享名。

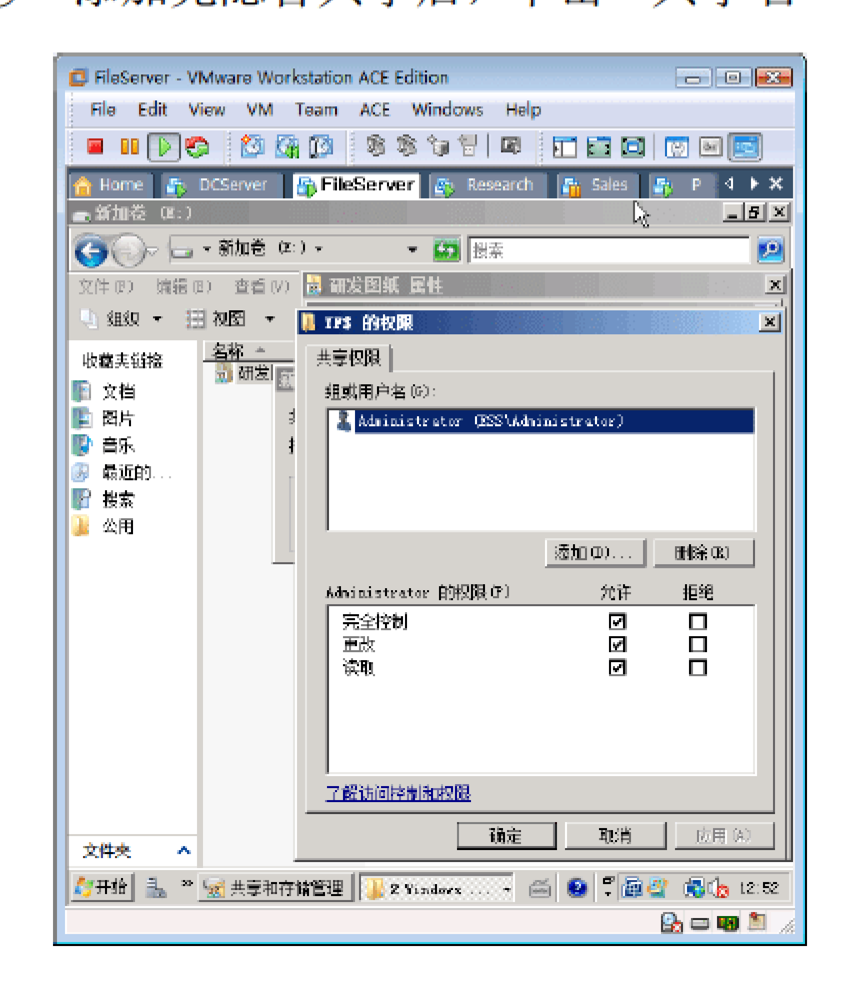


图 7-17　设置隐含共享的权限

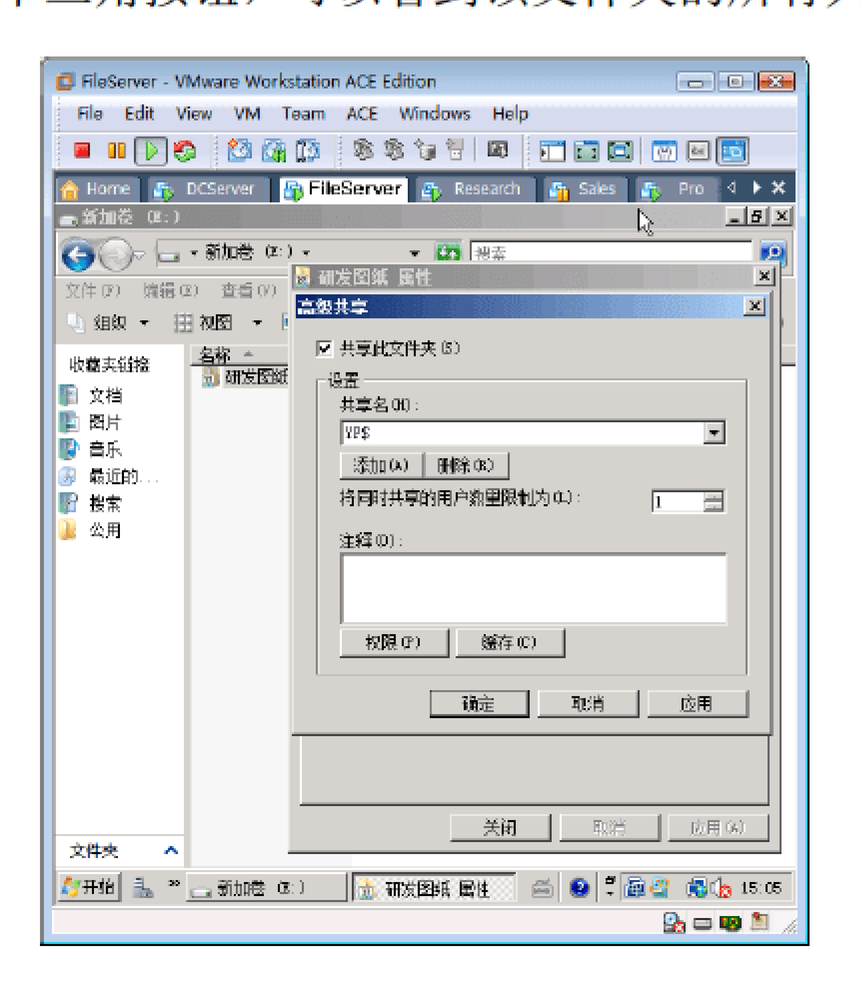


图 7-18　设置并发连接数

7.2.5　任务 5：管理本地计算机所有共享

查看服务器上的所有共享文件夹，包括隐含共享的文件。

①　选择“开始”→“程序”→“管理工具”→“共享和存储管理”命令。可以看到所有共享，包括隐含共享和默认共享：C$、E$、ADMIN$和 IPC$。

②　如图 7-19 所示，单击“设置共享”按钮，可以打开创建新的共享文件夹向导。

③　选中某个共享，单击“属性”按钮，可以更改共享的权限和 NTFS 权限以及并发连接的用户数量。

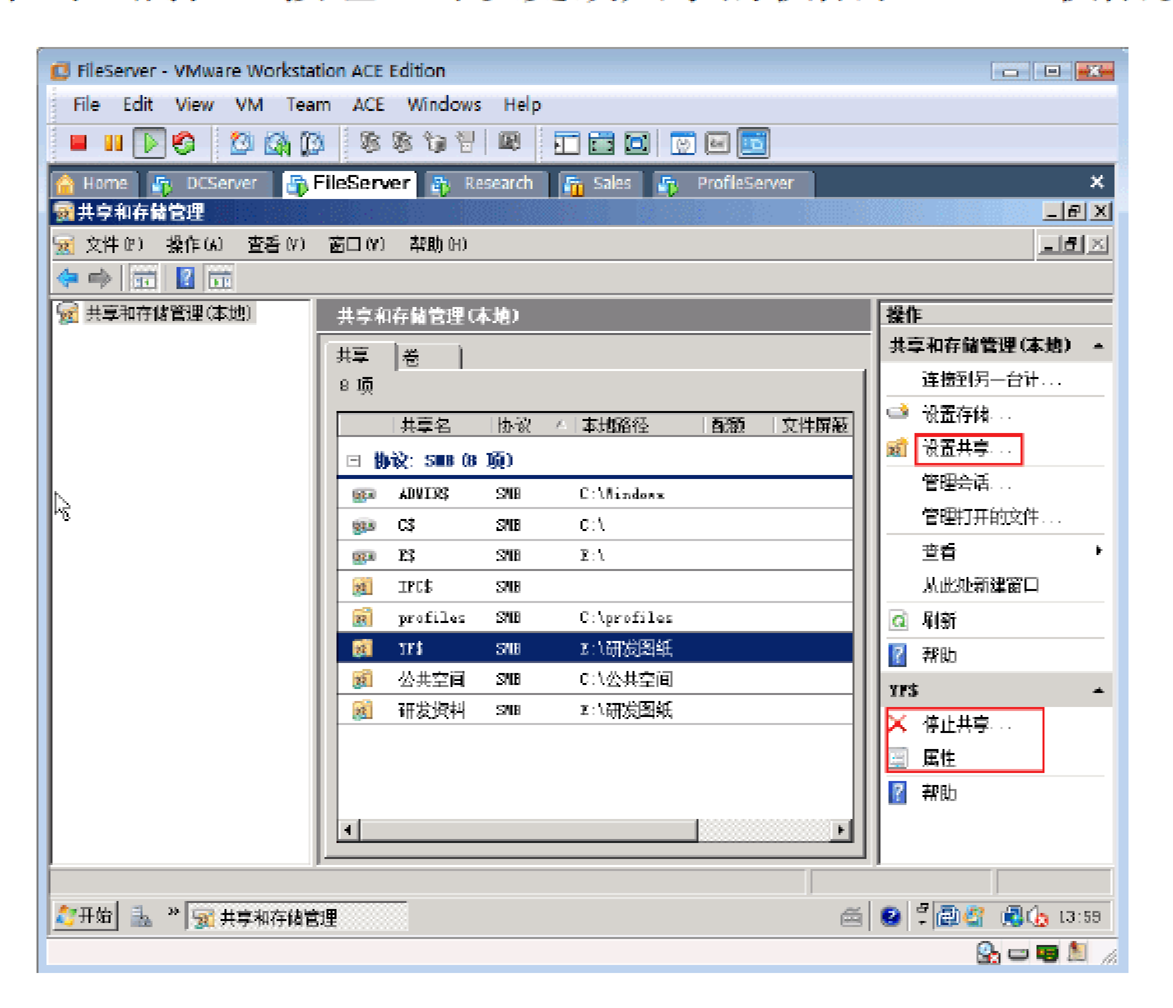
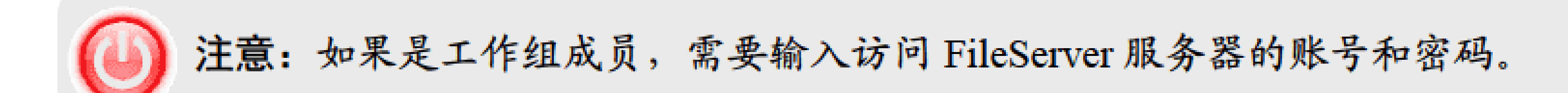


图 7-19　管理服务器所有共享

7.2.6 任务 6：访问服务器上共享资源和隐含共享资源

以域管理员的身份登录 Research 计算机访问 FileServer 计算机上共享的文件夹和隐含的共享。

① 如图 7-20 所示。选择“开始”→“运行”命令，输入“\\fileserver”，单击“确定”按钮。在出现的对话框中，可以看到 fileserver 上的共享文件夹，但是隐含共享的 YF$没有出现。



注意：如果是工作组成员，需要输入访问 FileServer 服务器的账号和密码。

② 如图 7-21 所示，选择“开始”→“运行”命令，输入“\\fileserver\yf$”，单击“确定”按钮，可以访问隐含的共享。

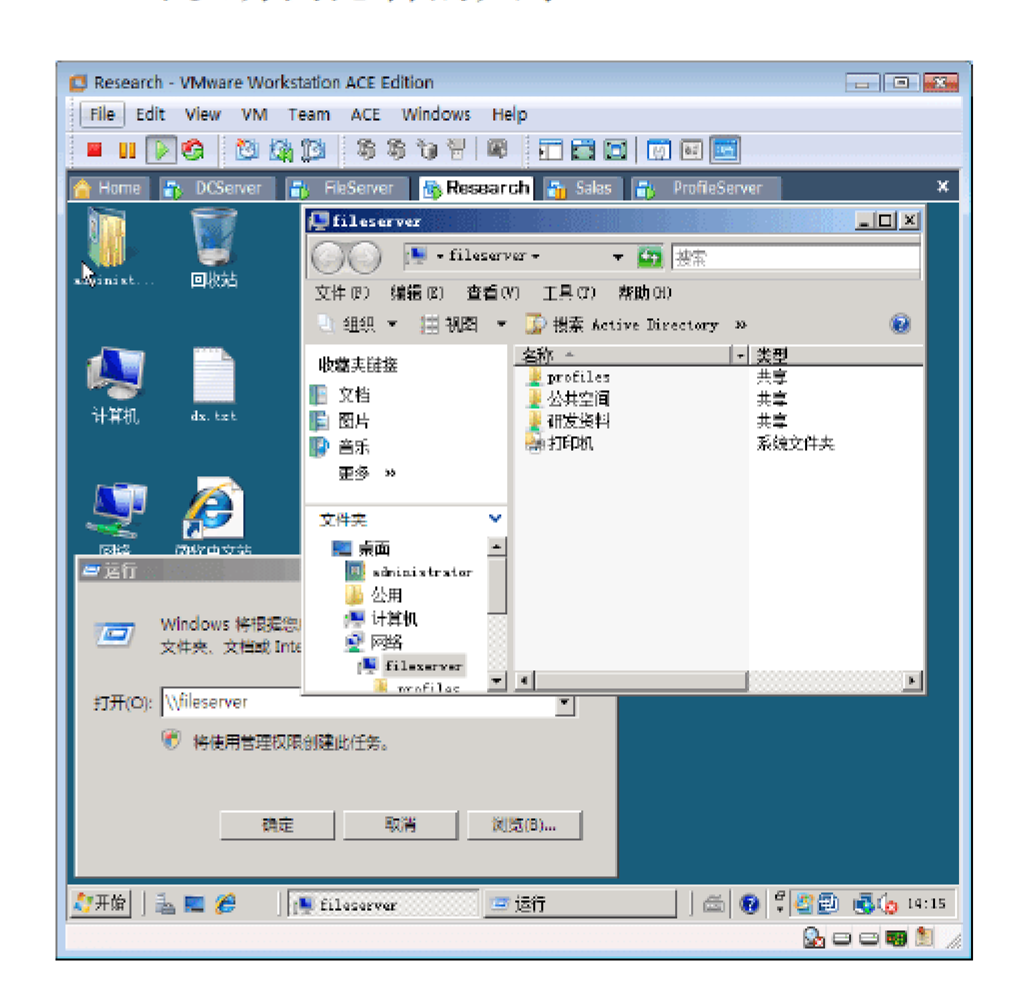



图 7-20 访问共享资源

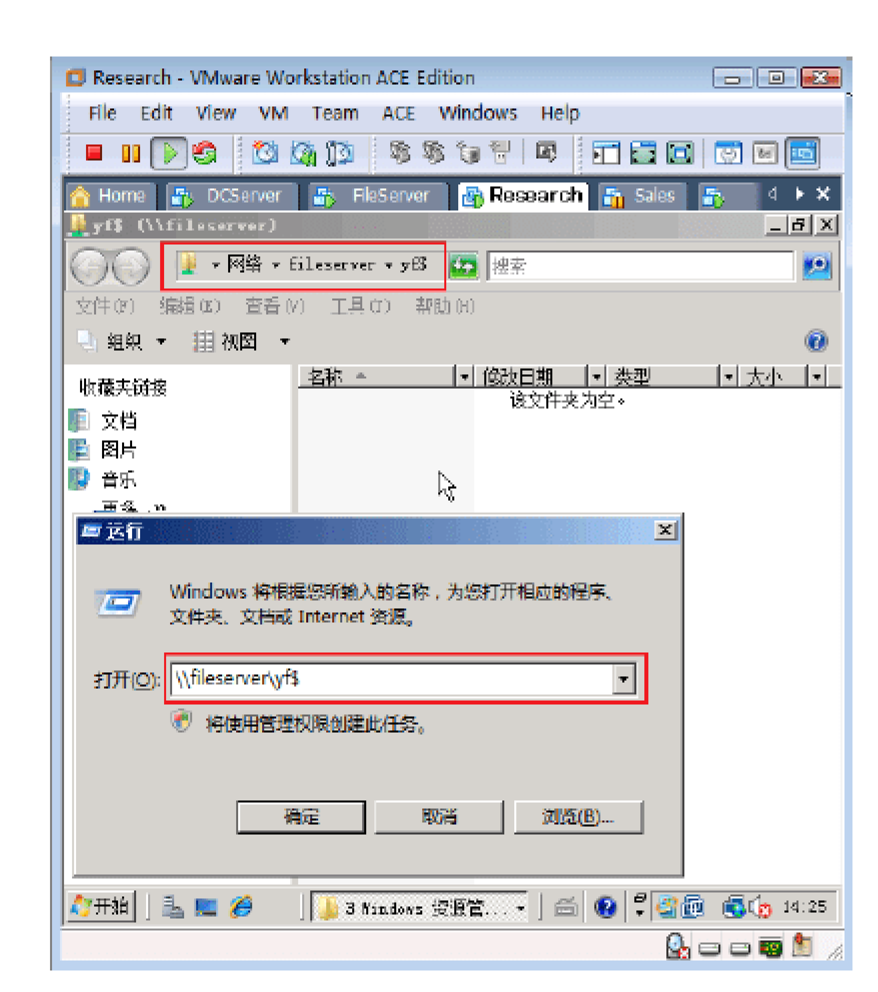


图 7-21 访问隐含共享

③ 如图 7-22 所示，直接在资源管理器中，输入“\\fileserver\yf$”，单击按钮也可以访问隐含共享的文件夹。

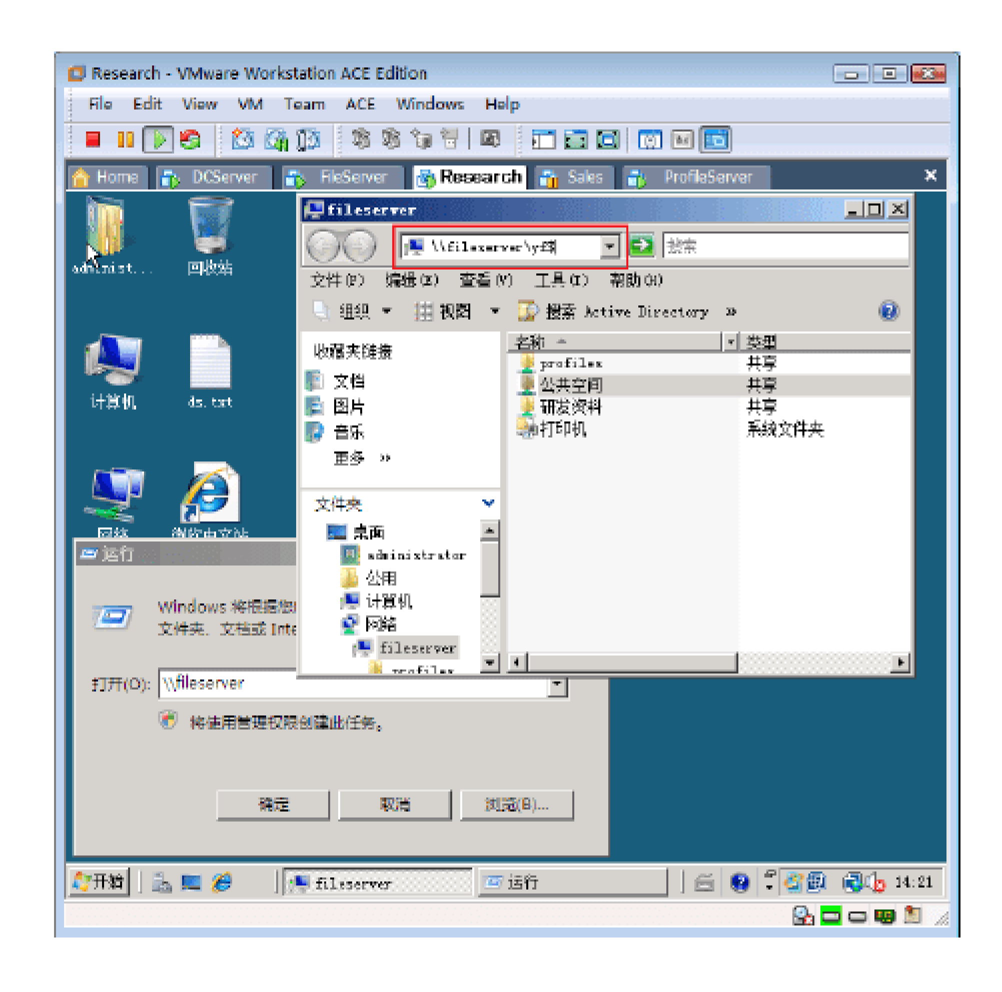


图 7-22 访问隐含共享

7.2.7　任务 7：访问默认共享

默认共享是为管理员管理服务器的方便而设的，其权限不能更改。只要知道服务器的管理员账号和密码，不管其是否明确共享了文件夹，你都可以访问其所有的分区。

在 Research 计算机上访问 FileServer 服务器的 C 盘

① 以域管理员的身份登录 Research 计算机。



注意：默认域管理员 Administrator 有域中所有计算机的管理员身份。

② 如图 7-23 所示，选择“开始”→“运行”命令，输入“\\fileserver\c$”，单击“确定”按钮，可以访问默认的共享。

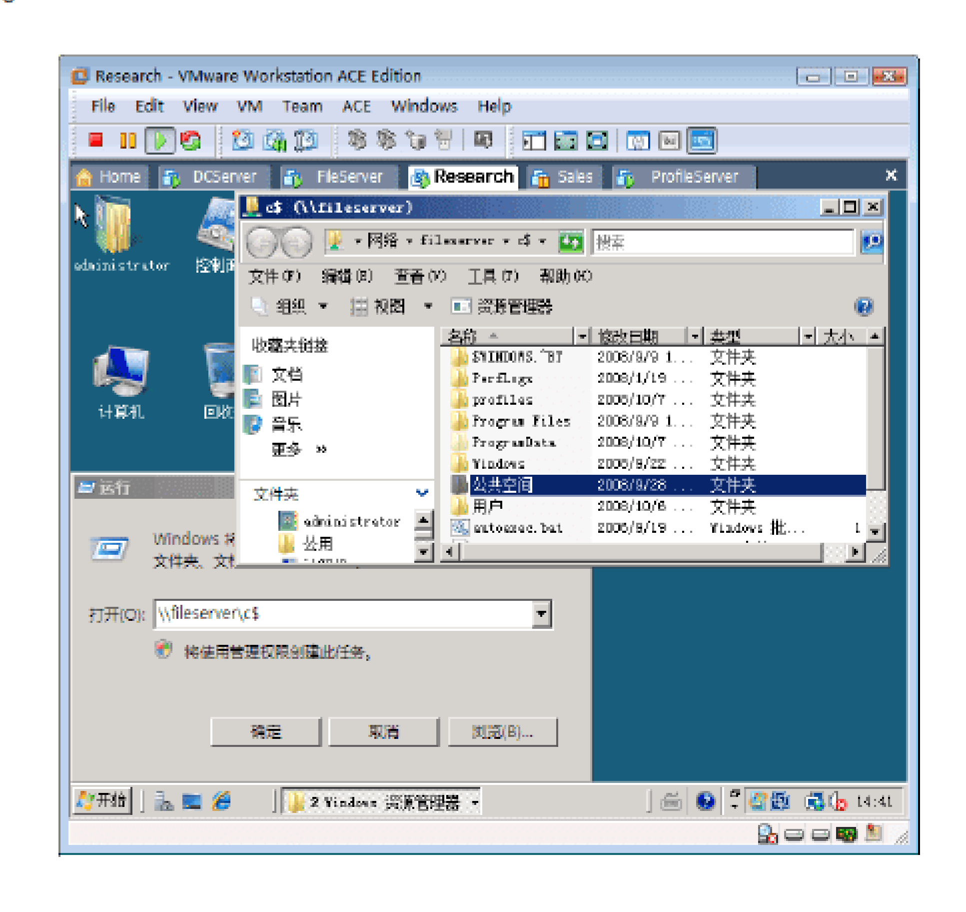


图 7-23　访问默认共享

7.2.8　任务 8：创建访问服务器资源的快捷方式

如果你经常访问 FileServer 服务器上的“研发资料”文件夹，可以将该文件夹映射成网络驱动器或创建访问该服务器共享资源的快捷方式。

示例 1：映射网络驱动器。

① 如图 7-24 所示，右击“研发资料”选项，在弹出的快捷菜单中选择“映射网络驱动器”命令。

② 在出现的如图 7-25 所示的对话框中，指定驱动器号，选中“登录时重新连接”复选框，单击“完成”按钮。

③ 双击桌面上的“计算机”图标，可以看到映射的网络驱动器，如图 7-26 所示。以后你就可以像访问本地磁盘一样访问服务器上的共享文件夹了。

示例 2：创建快捷方式。

可以在桌面上创建一个访问 FileServer 服务器共享资源的快捷方式。

① 如图 7-27 所示，右击桌面的空白位置，在弹出的快捷菜单中选择“快捷方式”→“新建”命令。

② 在出现的“创建快捷方式”对话框中，输入“\\fileserver”，如图 7-28 所示，单击“下一步”

按钮。

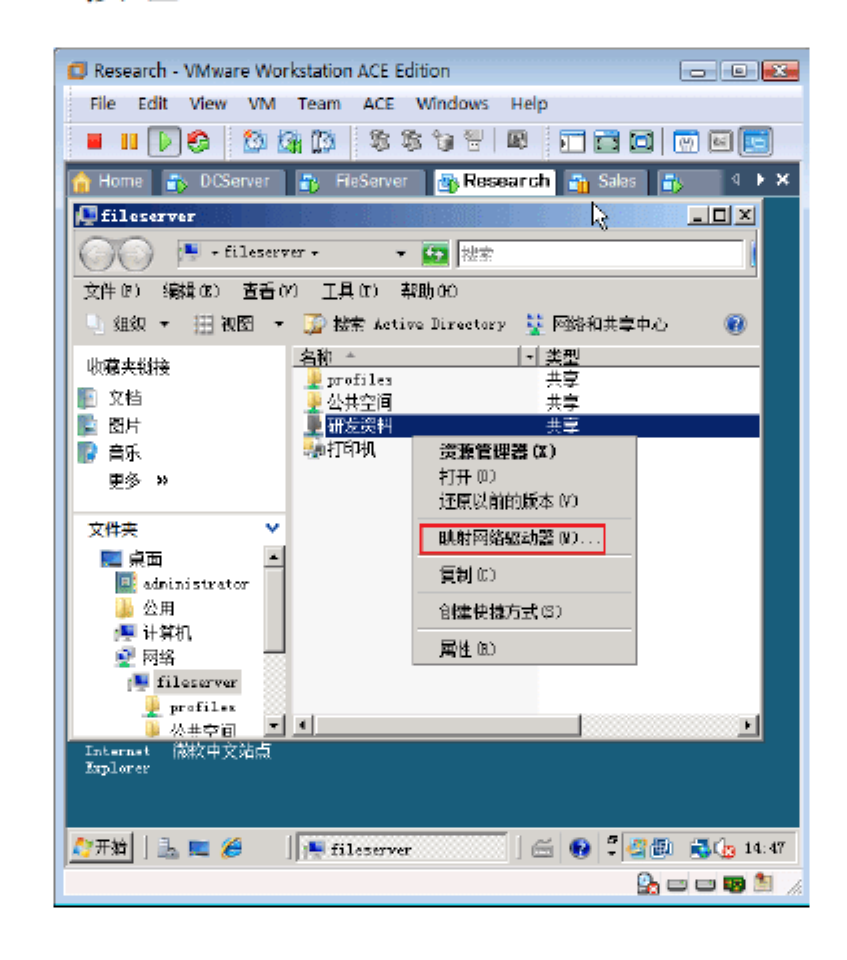


图 7-24　映射网络驱动器

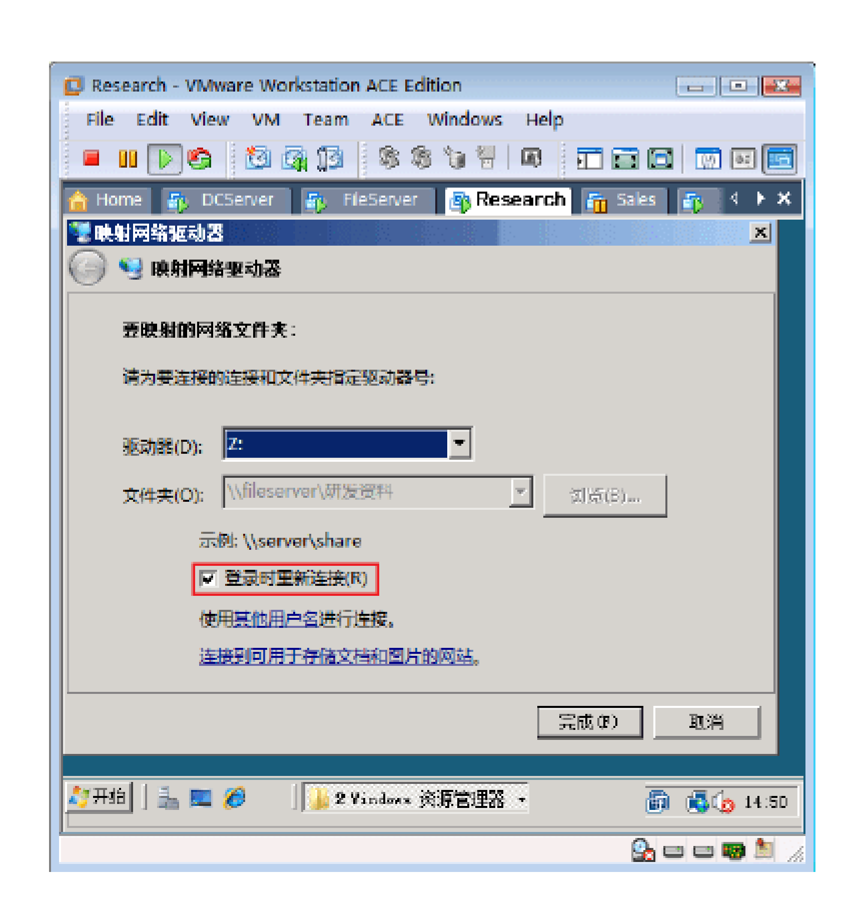


图 7-25　登录时自动连接

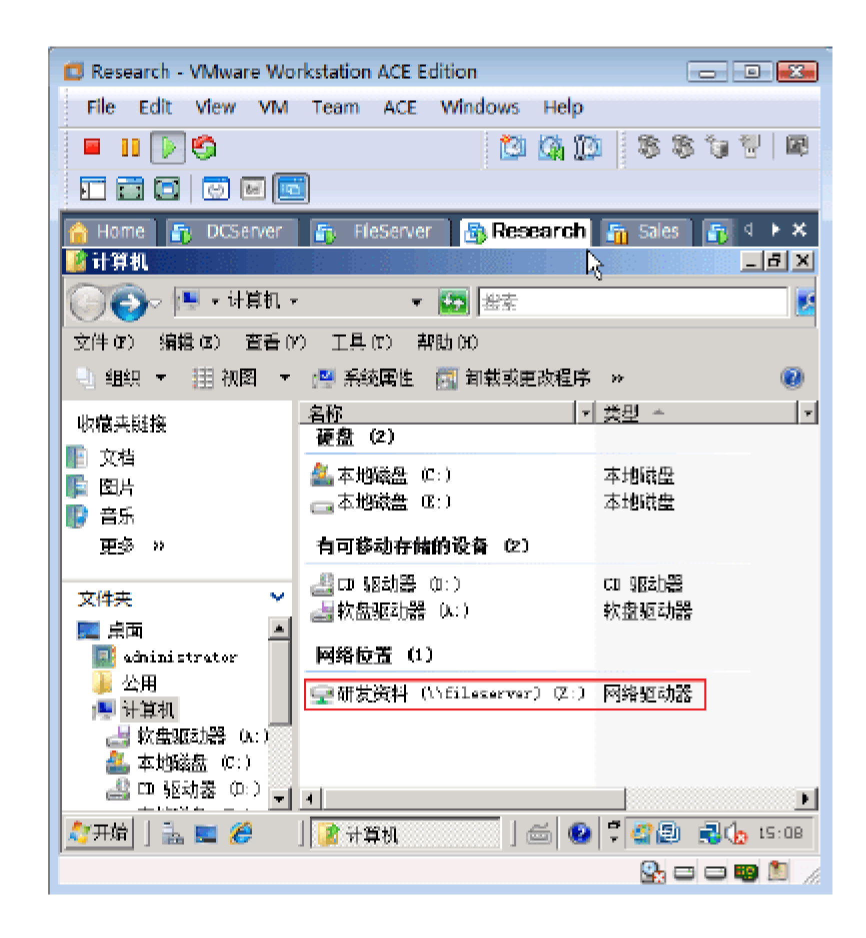


图 7-26　映射的网络驱动器

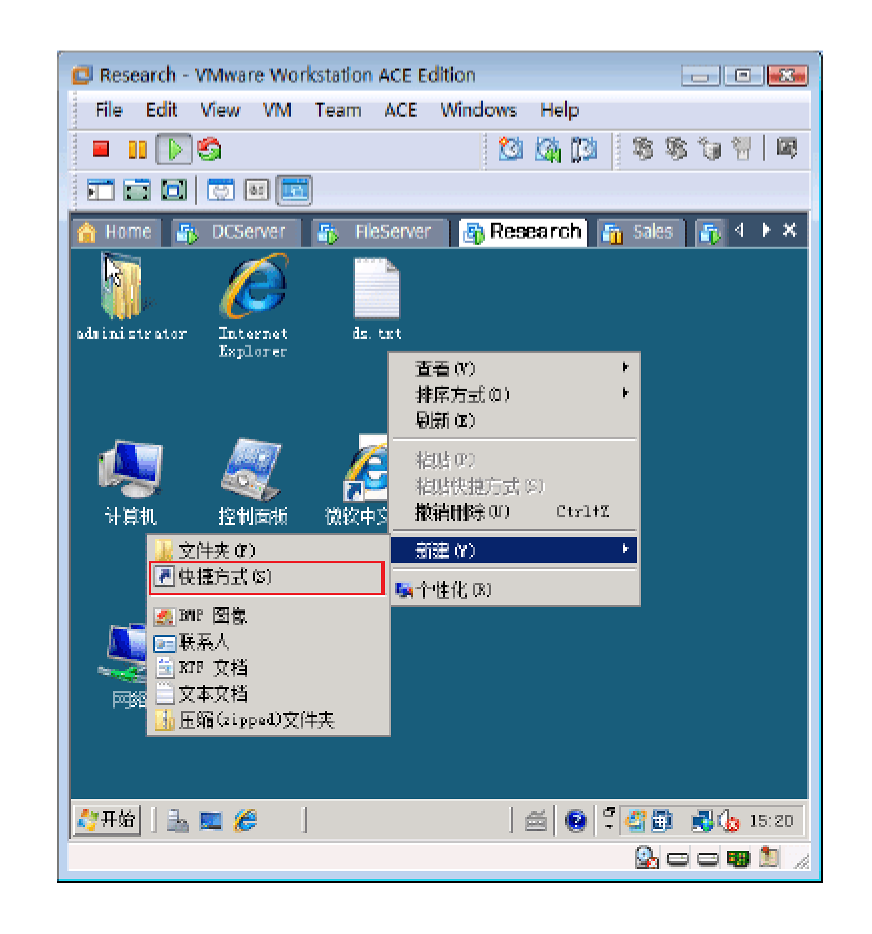


图 7-27　创建快捷方式

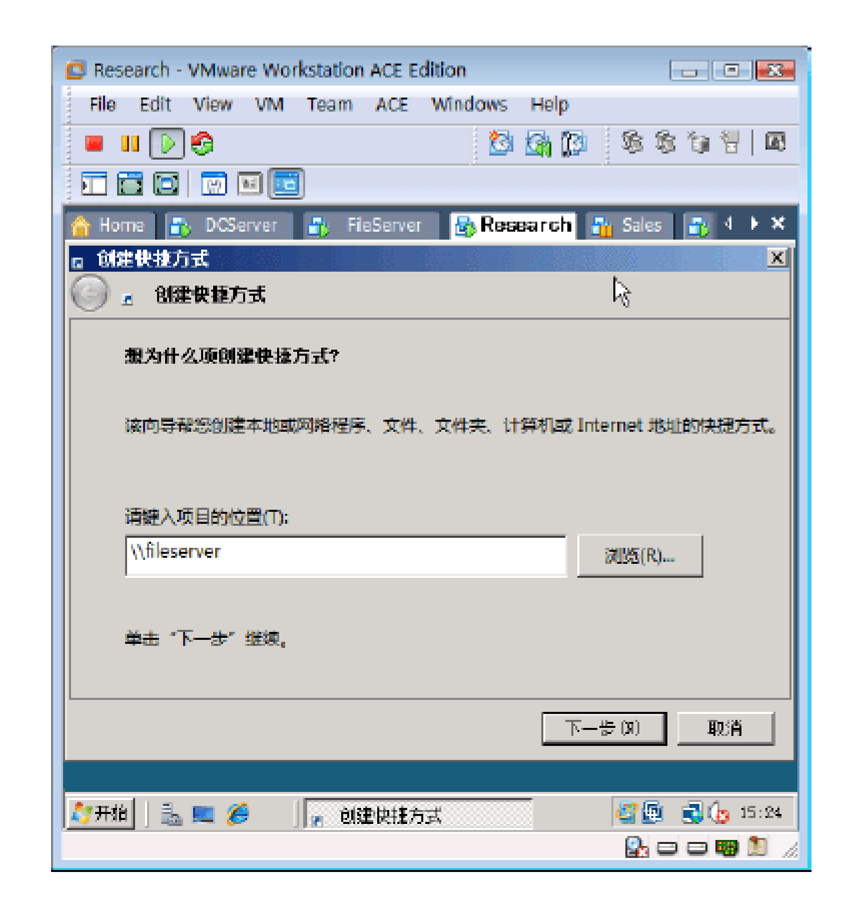


图 7-28　指定目标位置

③　输入快捷方式的名称，如图 7-29 所示，单击“完成”按钮。

④　可以看到创建的快捷方式，如图 7-30 所示。

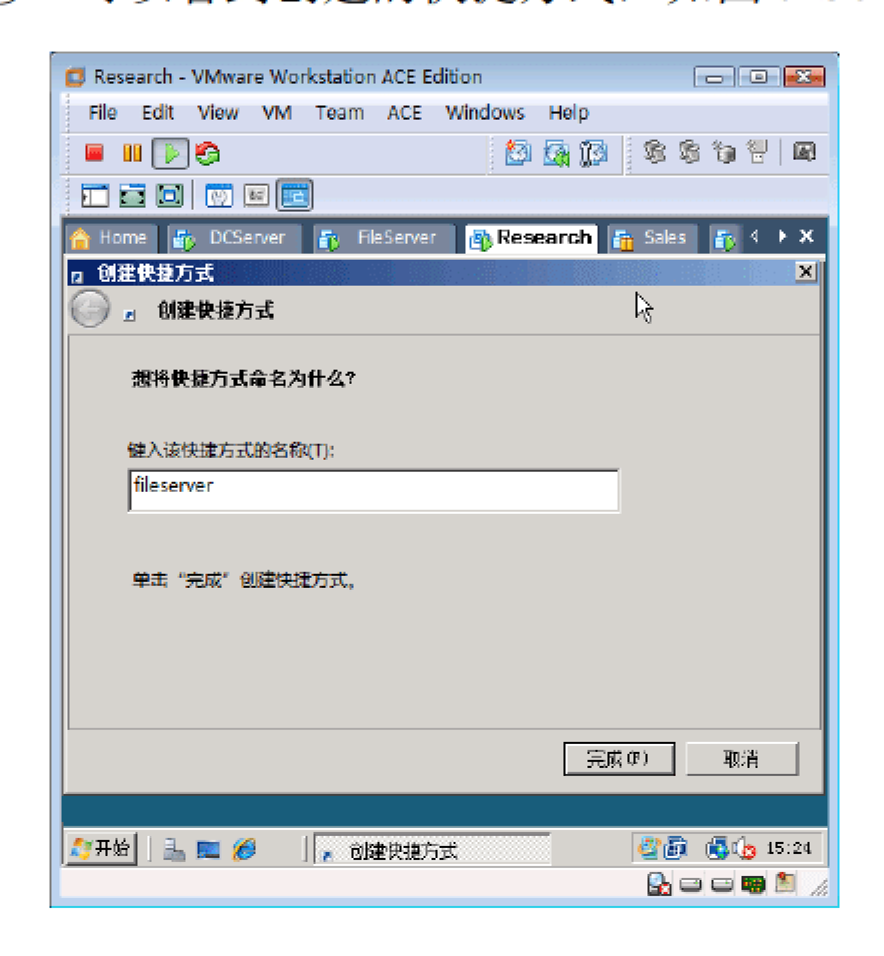


图 7-29　输入快捷方式的名称

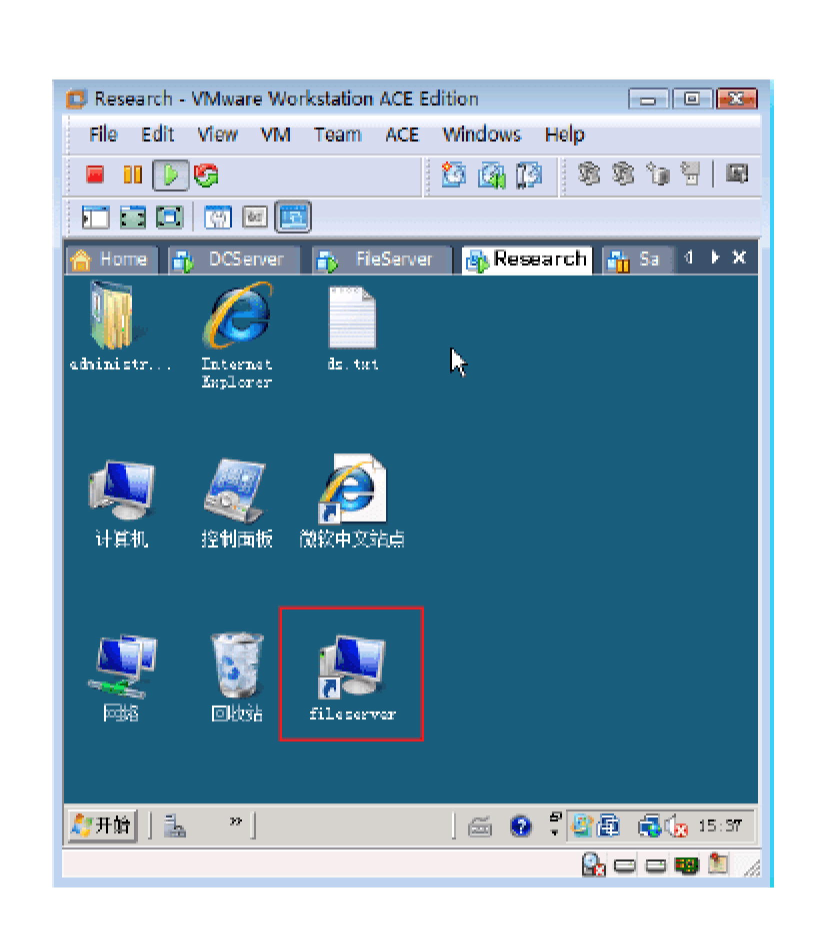


图 7-30　创建的快捷方式

7.2.9　任务 9：查看到文件服务器的会话

你可以在文件服务器上查看哪些用户正在访问哪些文件，也可以结束连接过来的用户访问。

示例：查看连接的会话。

①　选择“开始”→“程序”→“管理工具”→“共享和存储管理”命令。

②　如图 7-31 所示，在弹出的“共享和存储管理”对话框中，单击“管理会话”选项。

③　在出现的如图 7-32 所示的对话框中，可看到所有登录到 FileServer 服务器的用户。用户可以关闭会话。

④　如图 7-33 所示，在“管理打开的文件”对话框中，用户可以看到哪些用户正在访问哪些文件。

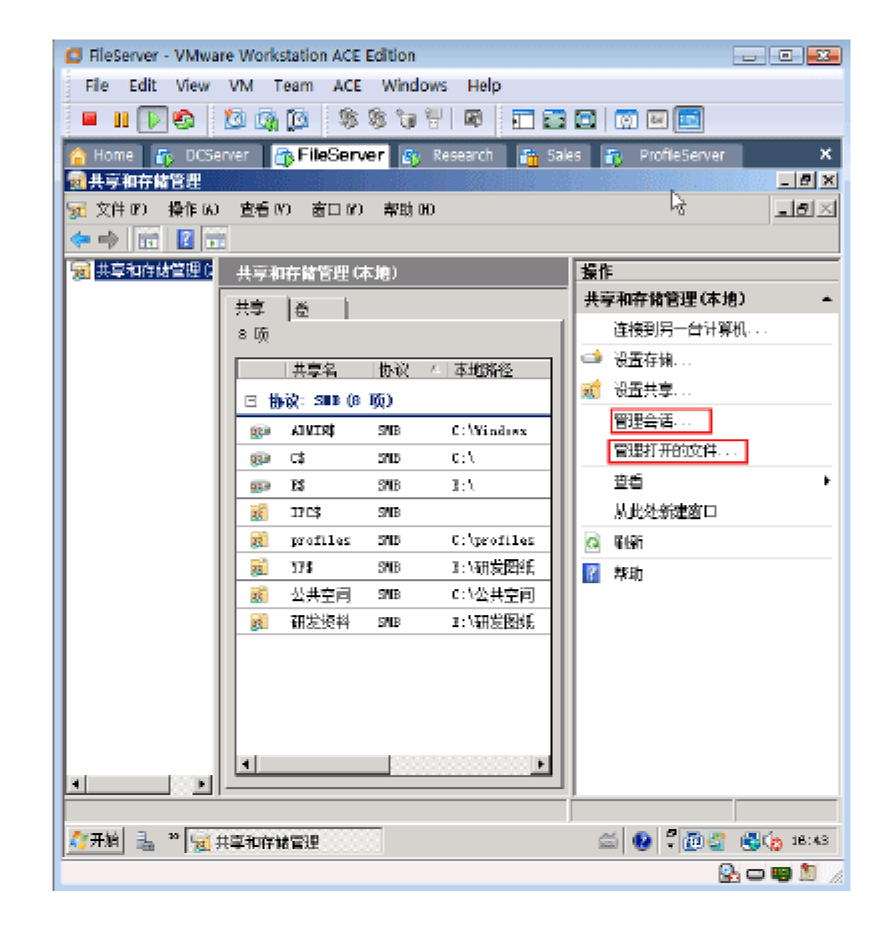


图 7-31　管理会话

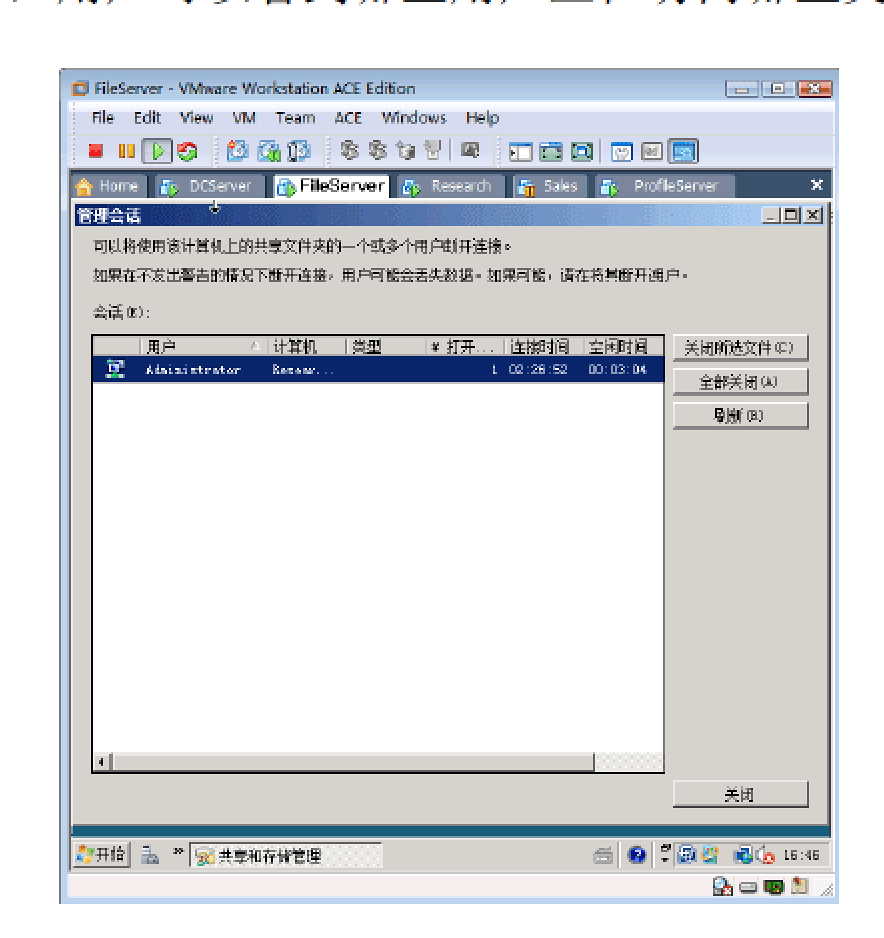


图 7-32　查看会话

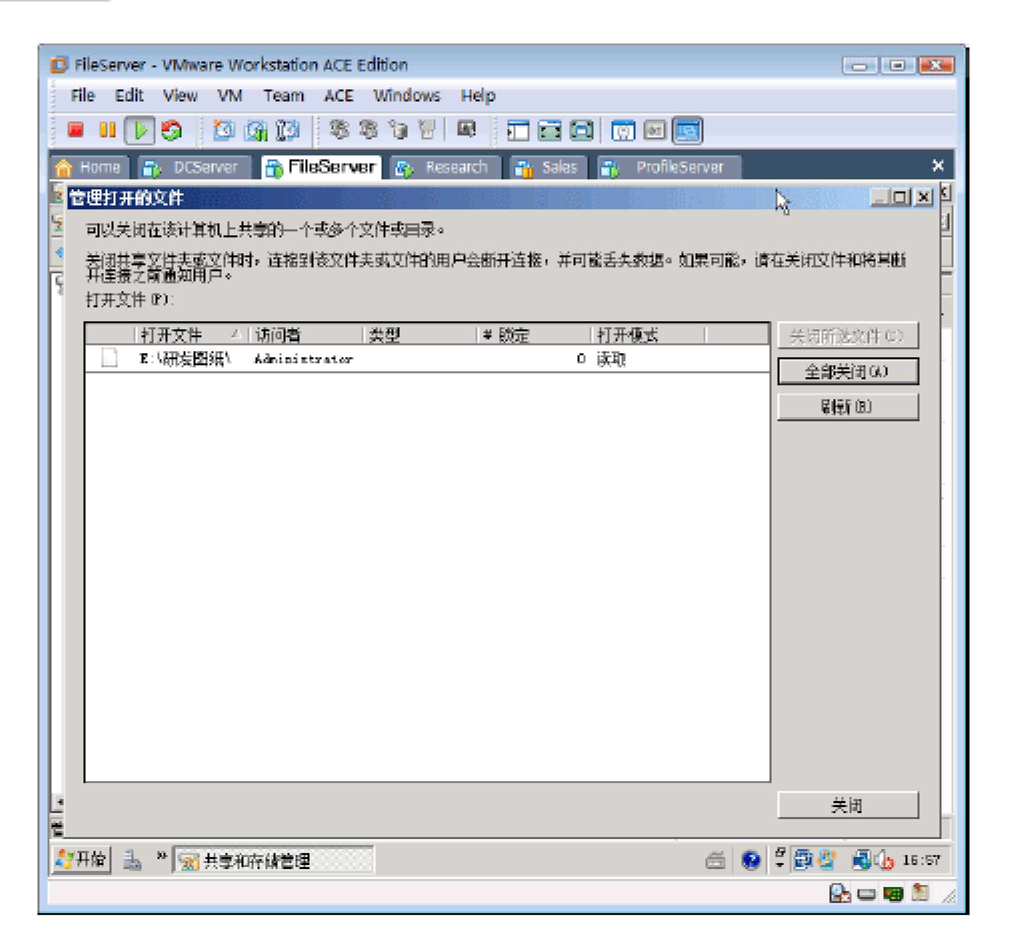


图 7-33　查看打开的文件

7.2.10　任务 10：管理 Windows Server Core 服务器共享文件夹

Windows Server Core 没有图形界面，使用命令管理其共享文件、设置 NTFS 权限和共享权限较为复杂，现在介绍一种图形化的管理工具，远程管理 Windows Server Core 服务器上的共享文件夹。

示例：管理 Windows Server Core 服务器上的共享文件夹。

使用 FileServer 上的管理工具管理装了 Windows Server Core 操作系统的 ProfileServer 上的共享文件。

① 以域管理员的用户账户登录 FileServer 服务器。

② 选择“开始”→“程序”→“管理工具”→“共享和存储管理”命令。

③ 单击“连接到另一台计算机”按钮，在出现的对话框中，选中“另一台计算机”单选按钮，在文本框中输入 ProfileServer，如图 7-34 所示。单击“确定”按钮。

④ 现在管理工具连接到了 ProfileServer，如图 7-35 所示。单击“设置共享”按钮。

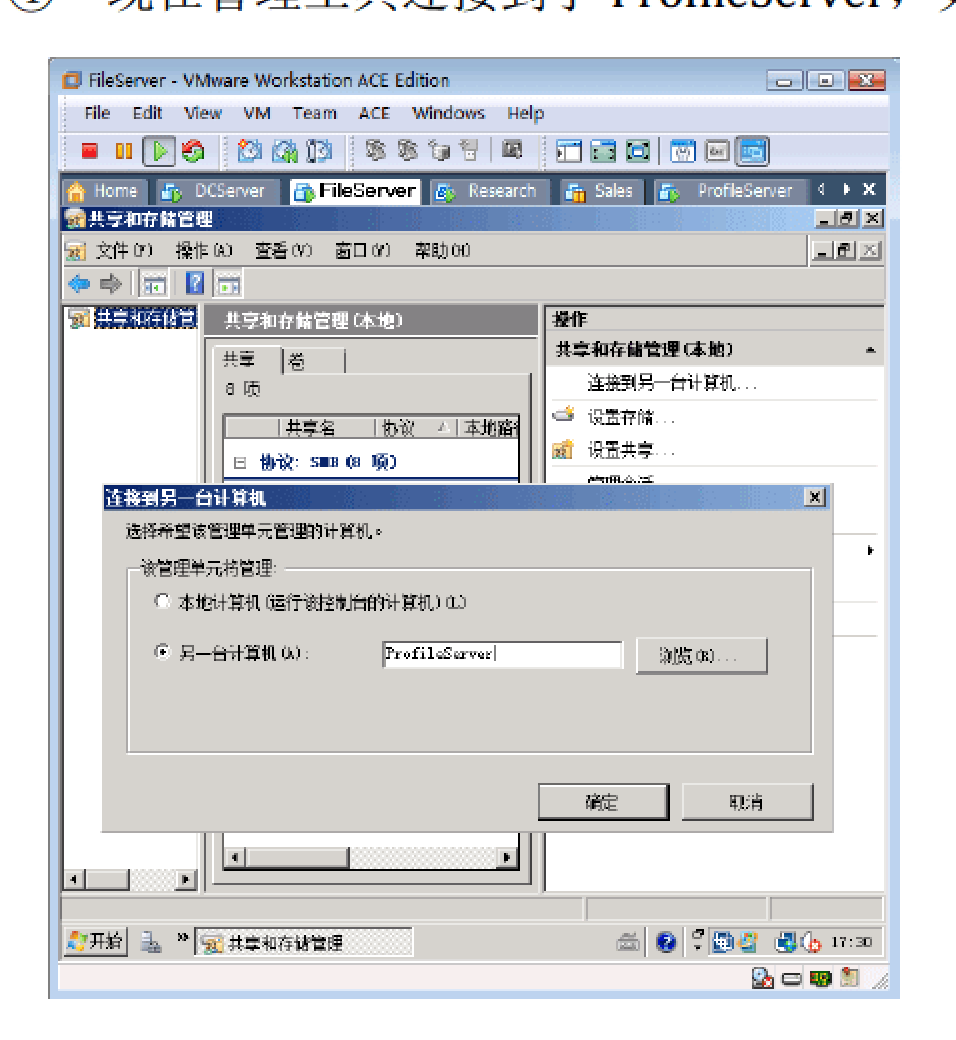


图 7-34　连接到 Server Core

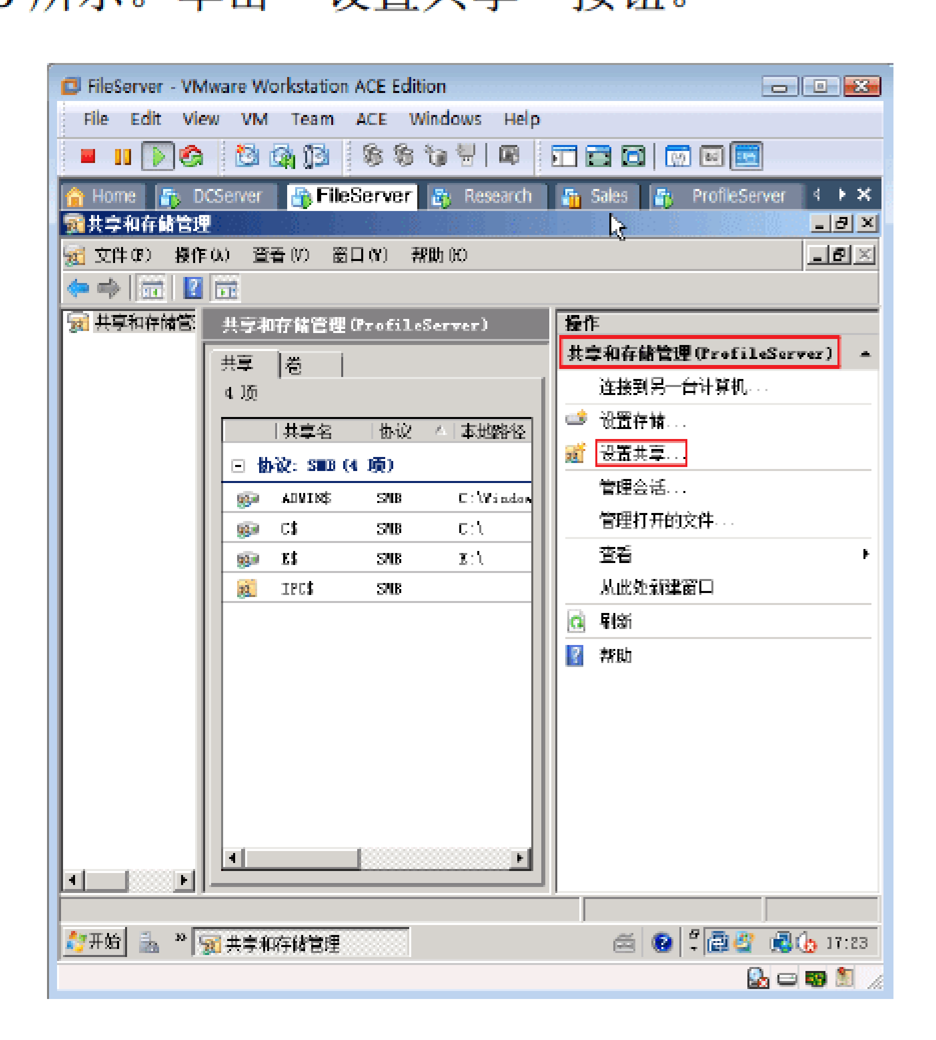


图 7-35　可以设置共享

⑤　如图 7-36 所示，在“共享文件夹位置”界面中，单击“浏览”按钮。

⑥　如图 7-37 所示，在出现的“浏览文件夹”对话框中，在 E$下创建一个文件夹“研发图纸”。选中该文件夹，单击“确定”按钮，再单击“下一步”按钮。

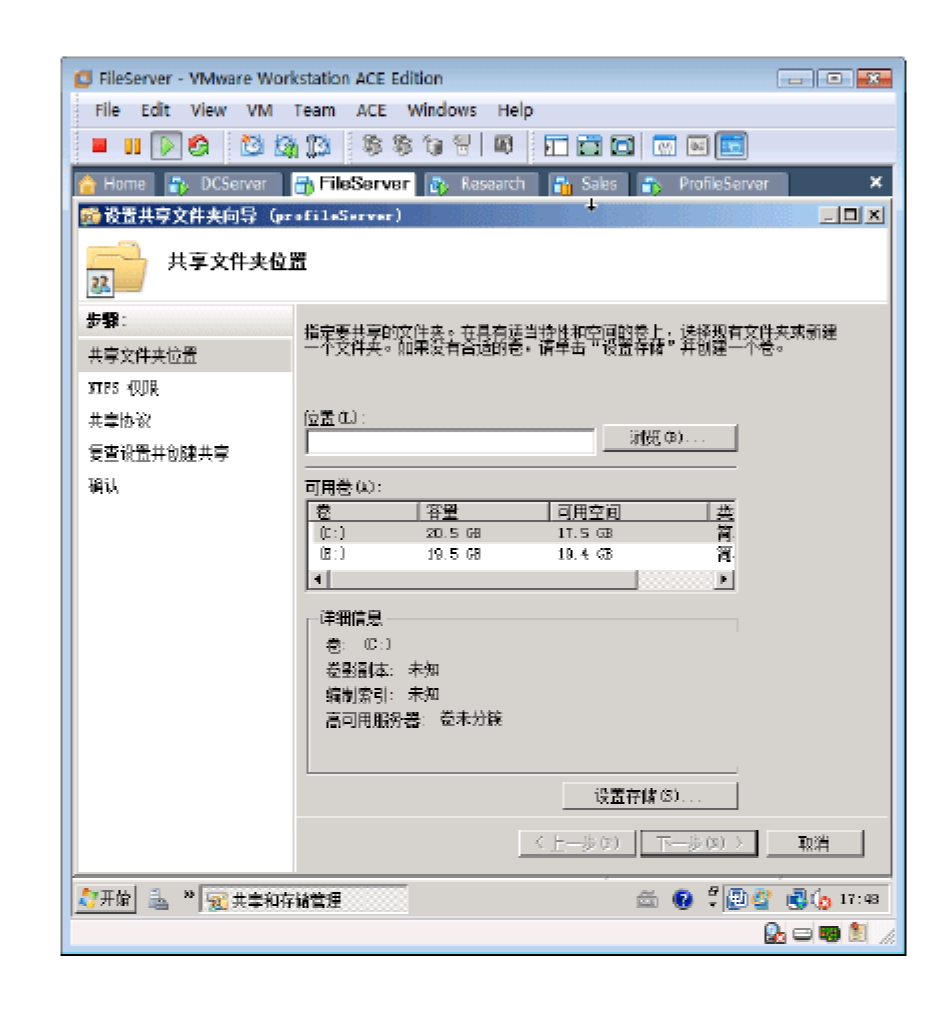


图 7-36　浏览要共享的文件夹

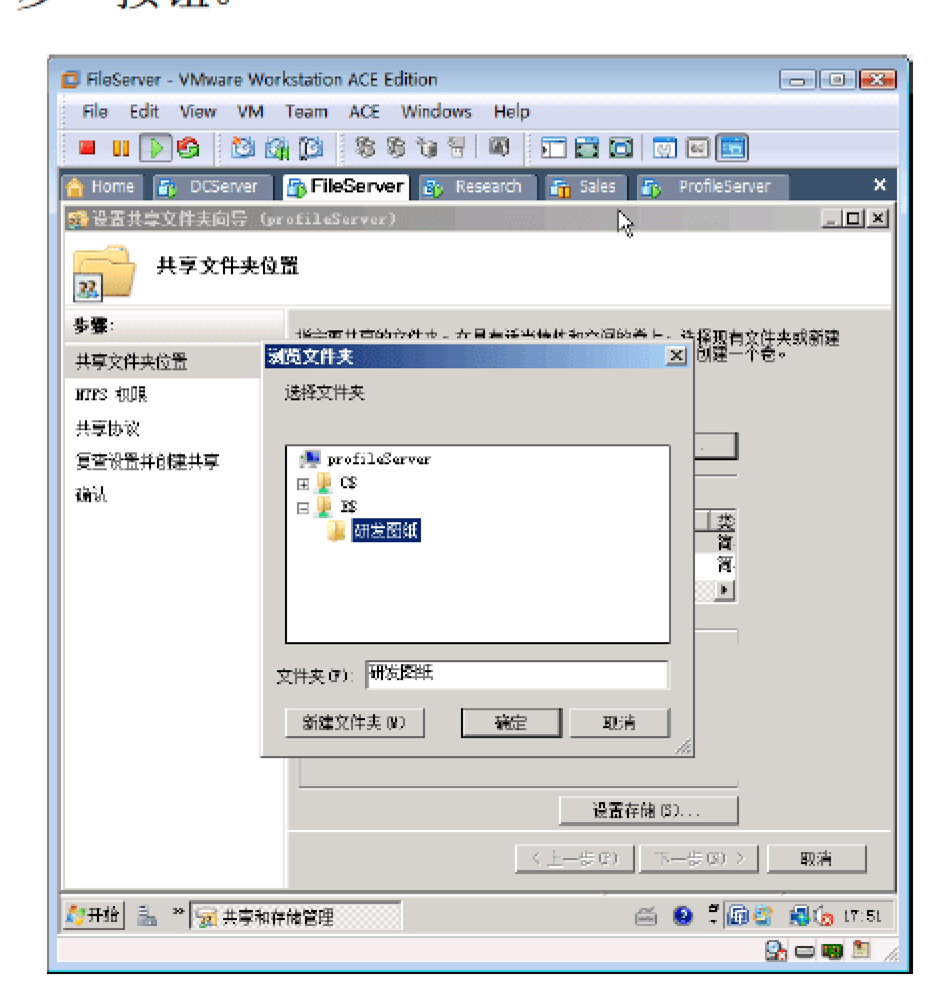


图 7-37　新建要共享的文件夹

⑦　如图 7-38 所示，在出现的“NTFS 权限”界面中单击“下一步”按钮。

⑧　如图 7-39 所示，在出现的“共享协议”界面中，默认选中 SMB，共享名默认为文件夹的名称，单击“下一步”按钮。

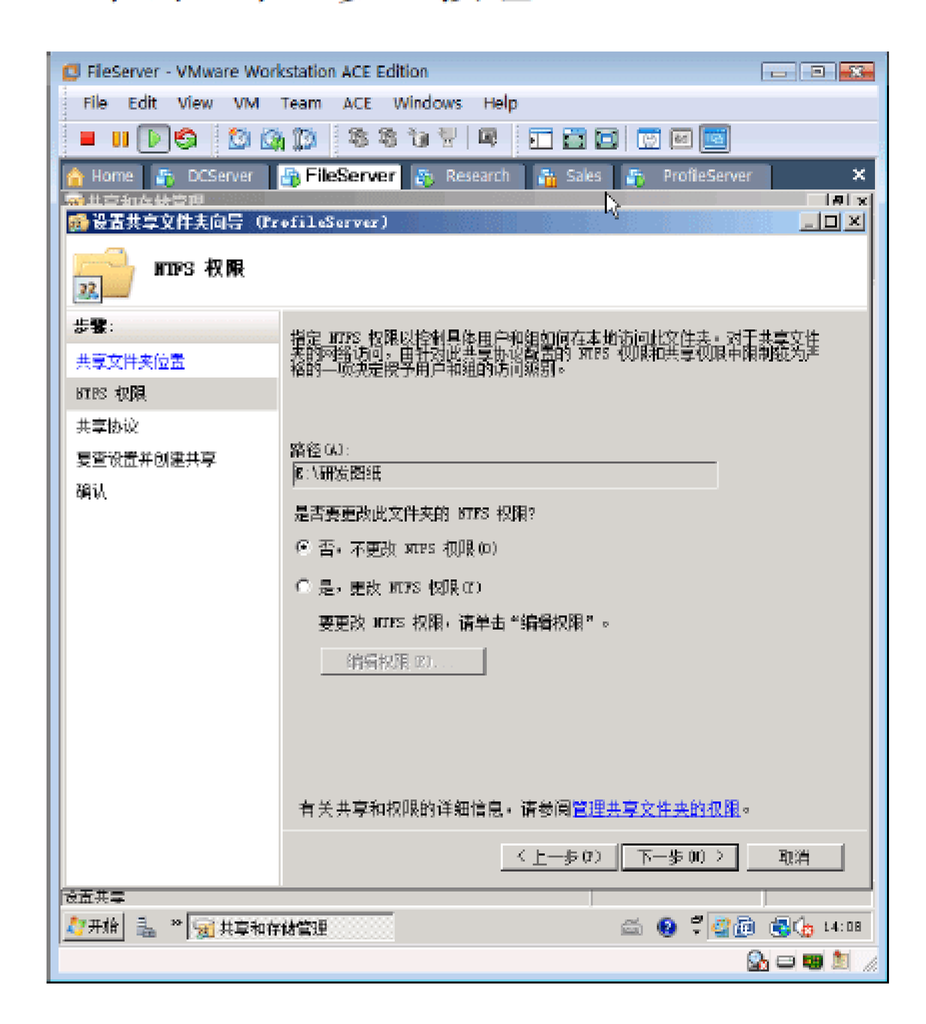


图 7-38　设置 NTFS 权限

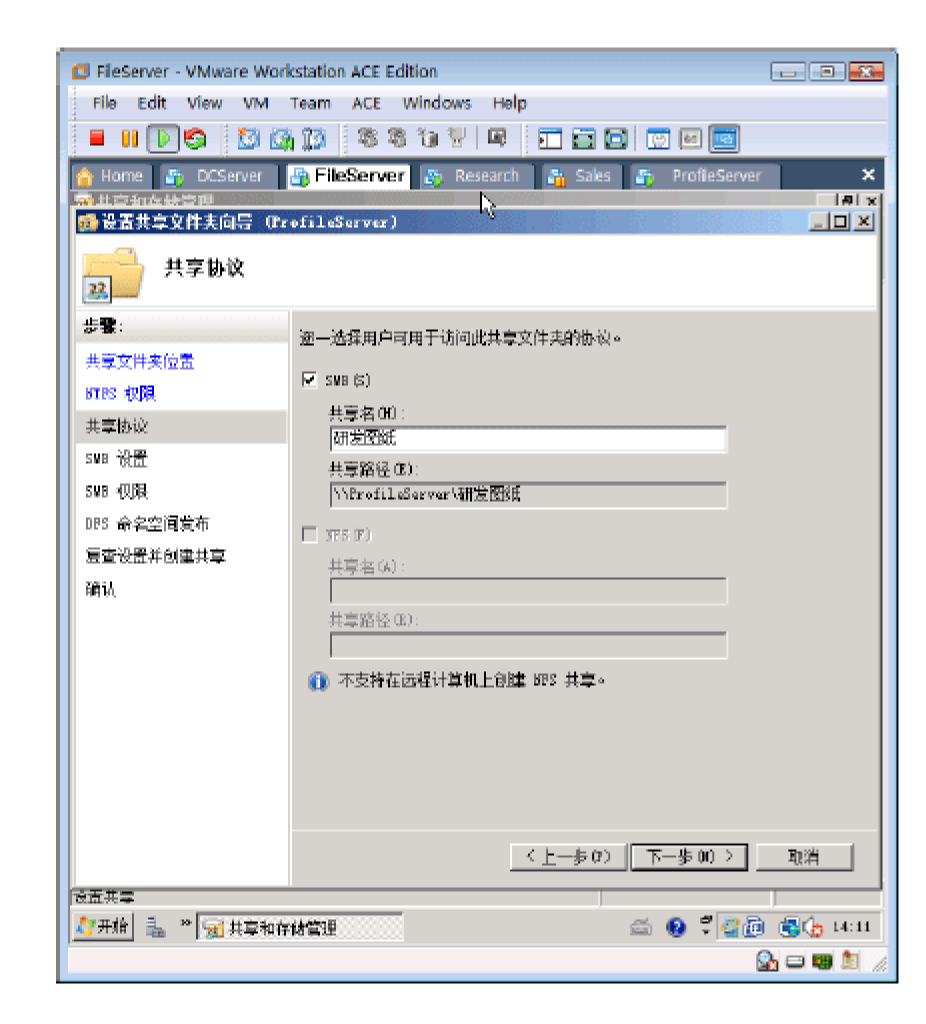


图 7-39　指定共享名

⑨　如图 7-40 所示，在出现的“SMB 设置”界面中单击“高级”，设置用户限制，单击“确定”按钮。

⑩　如图 7-41 所示，在出现的“SMB 权限”界面中单击“权限”，删掉 Everyone 的访问权限，添加“研发人员”能够读取和更改的共享权限。单击“下一步”按钮。

⑪　如图 7-42 所示，在出现的“DFS 命名空间发布”界面中单击“下一步”按钮，完成共享设置。

⑫ 如图 7-43 所示，选中刚才创建的共享文件夹，选择“属性”，在“研发图纸 属性”对话框的“权限”选项卡下，可以设置 NTFS 权限和共享权限。

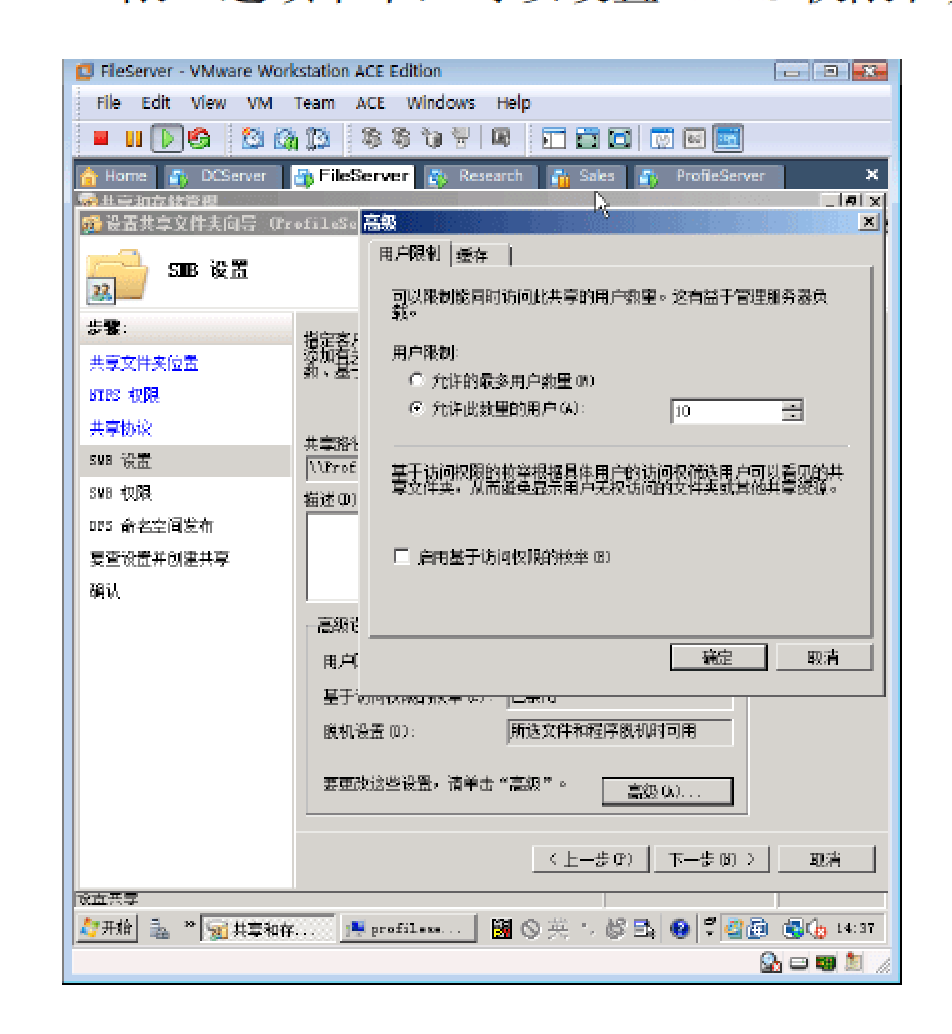


图 7-40　设置并发连接数

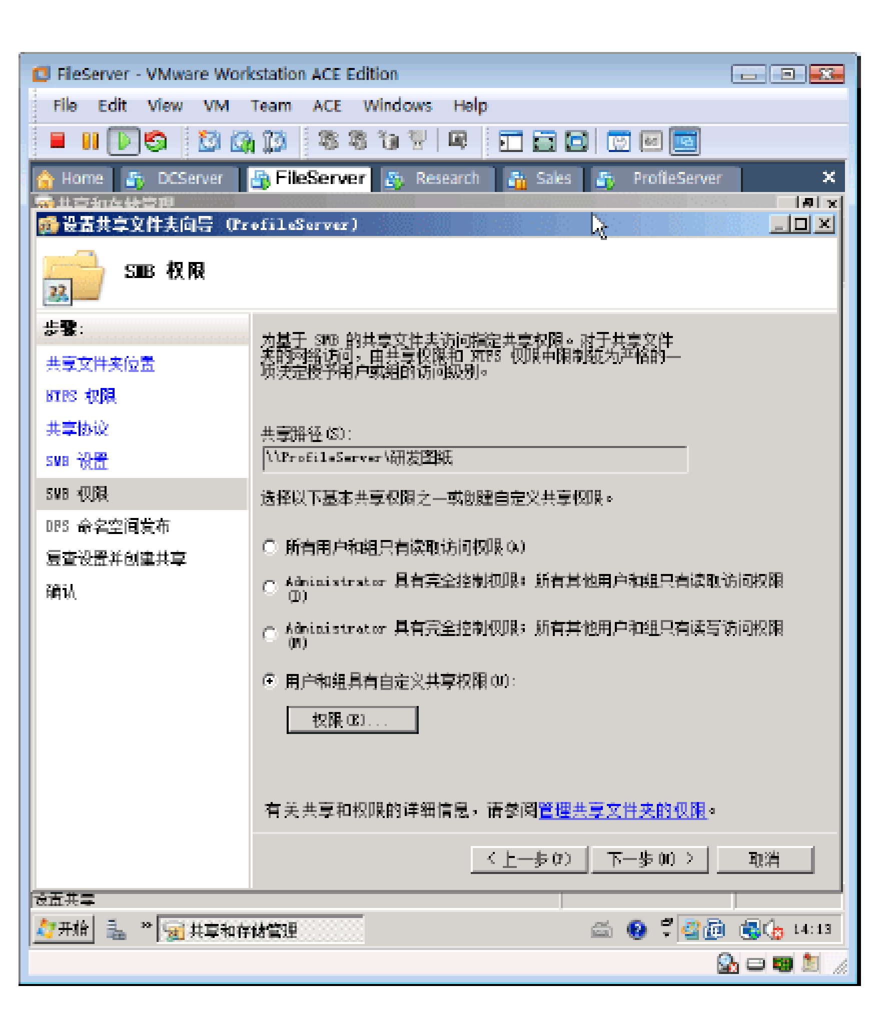


图 7-41　设置共享权限

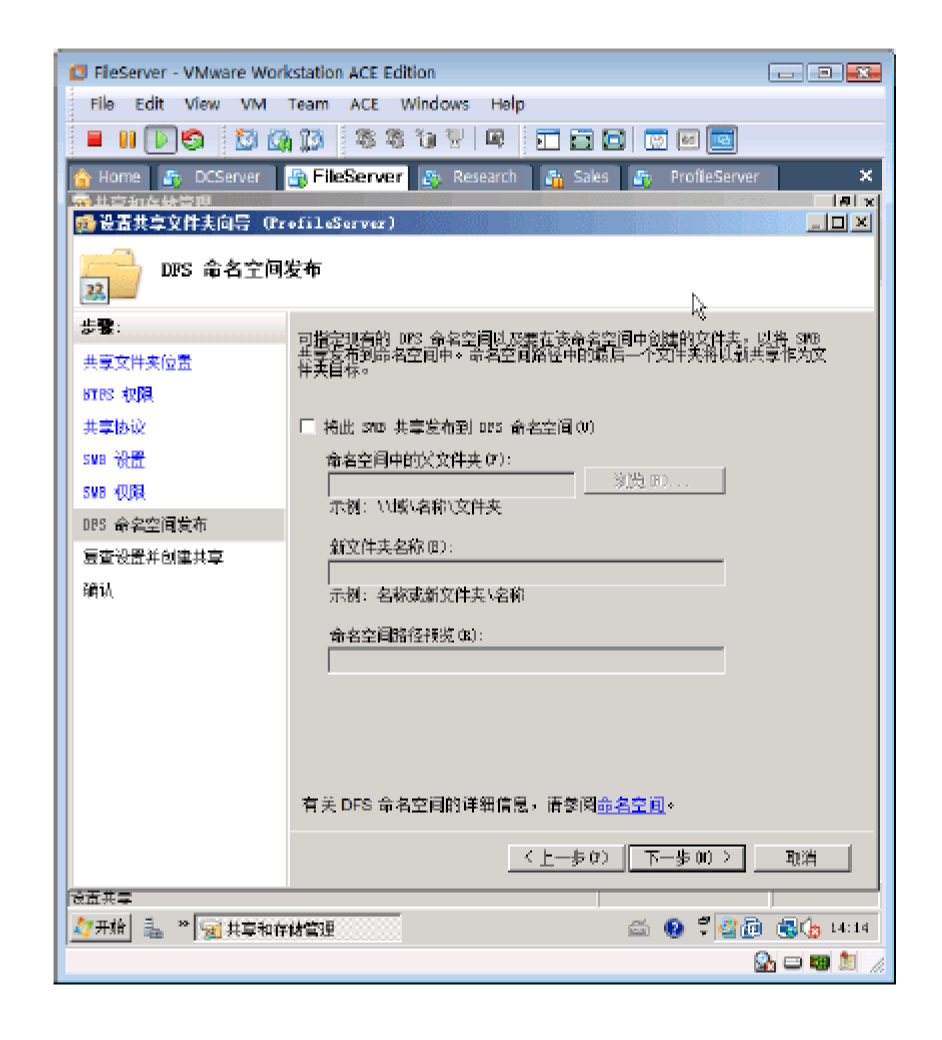


图 7-42　DFS 命名空间发布

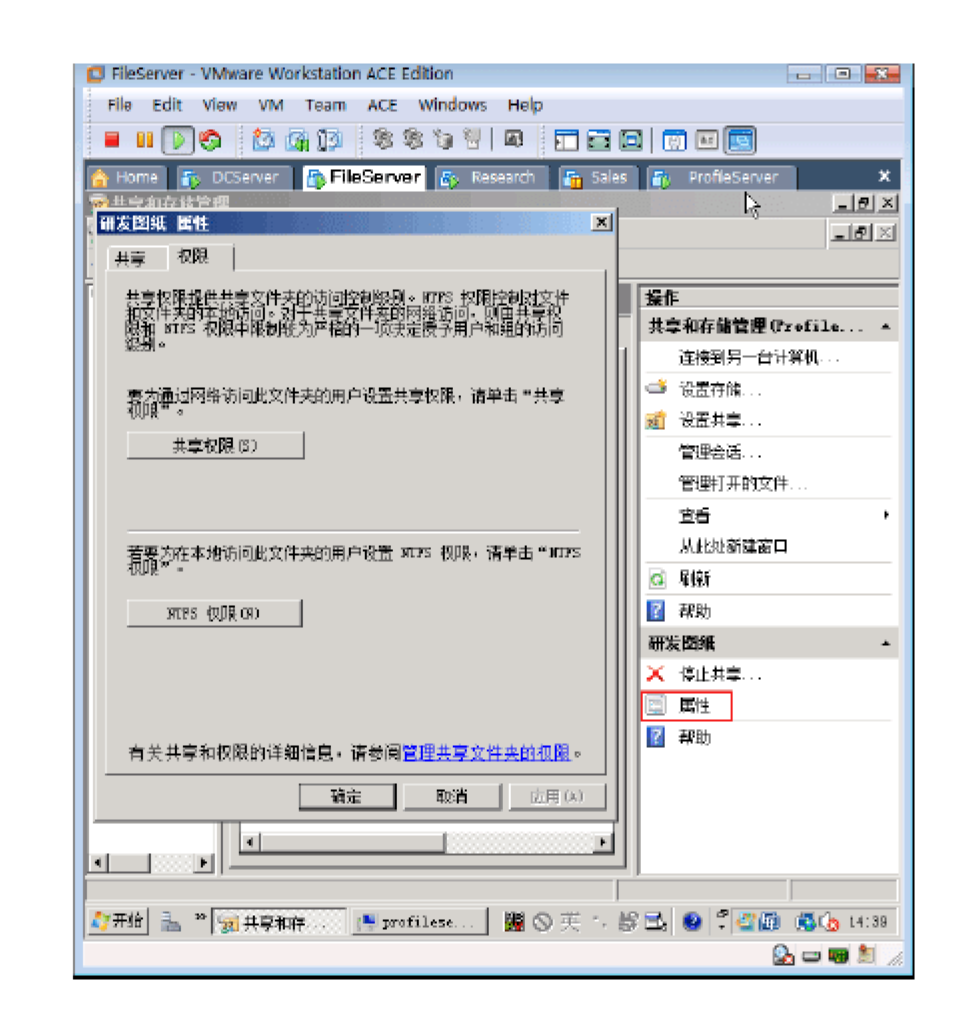


图 7-43　设置共享权限和 NTFS 权限

7.2.11　任务 11：去掉默认共享

为了安全起见，可以考虑将服务器上的默认共享禁止。

示例：去掉默认共享。

① 选择“开始”→“运行”命令，输入 regedit，单击“确定”按钮。

② 如图 7-44 所示，打开注册表编辑器。在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters 下新建 REG_DWORD 值。名称输入：AutoShareServer。

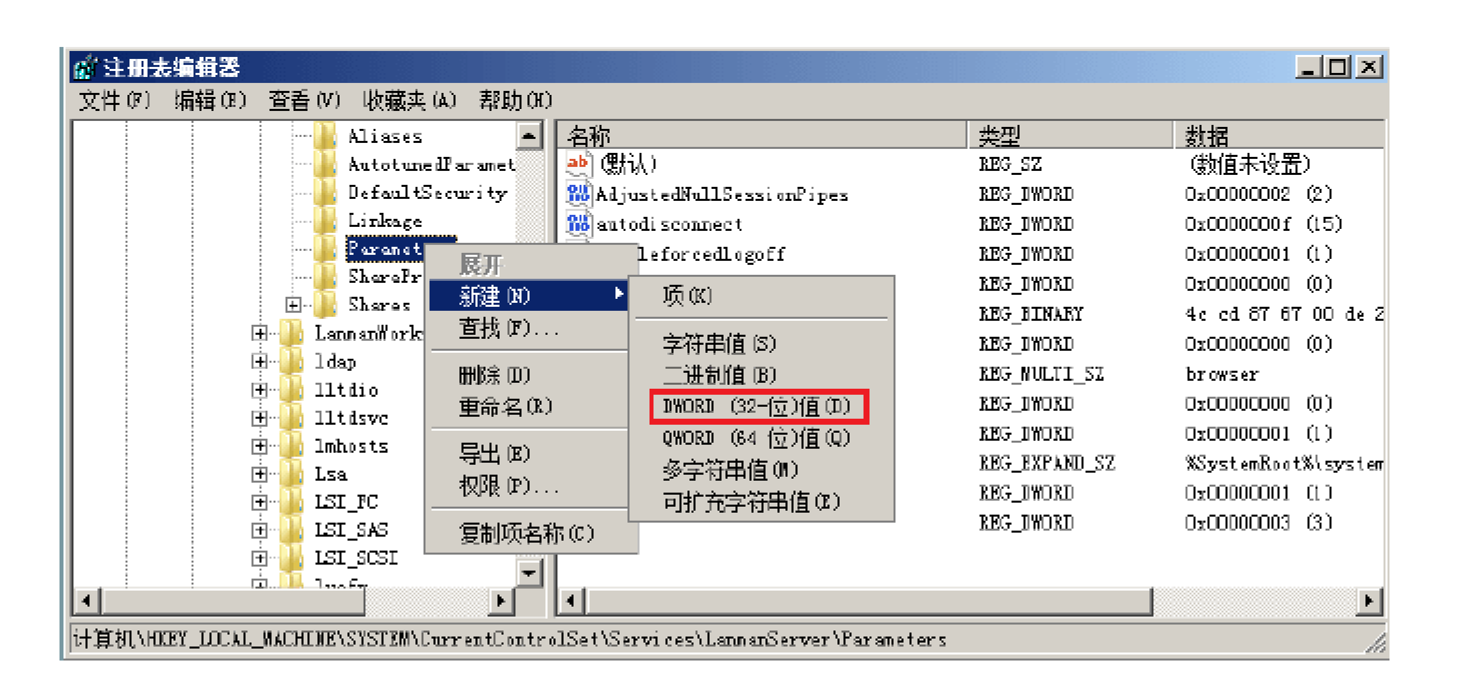


图 7-44　创建键值

③　如图 7-45 所示，双击刚才创建的项，输入数值为 0，单击“确定”按钮。

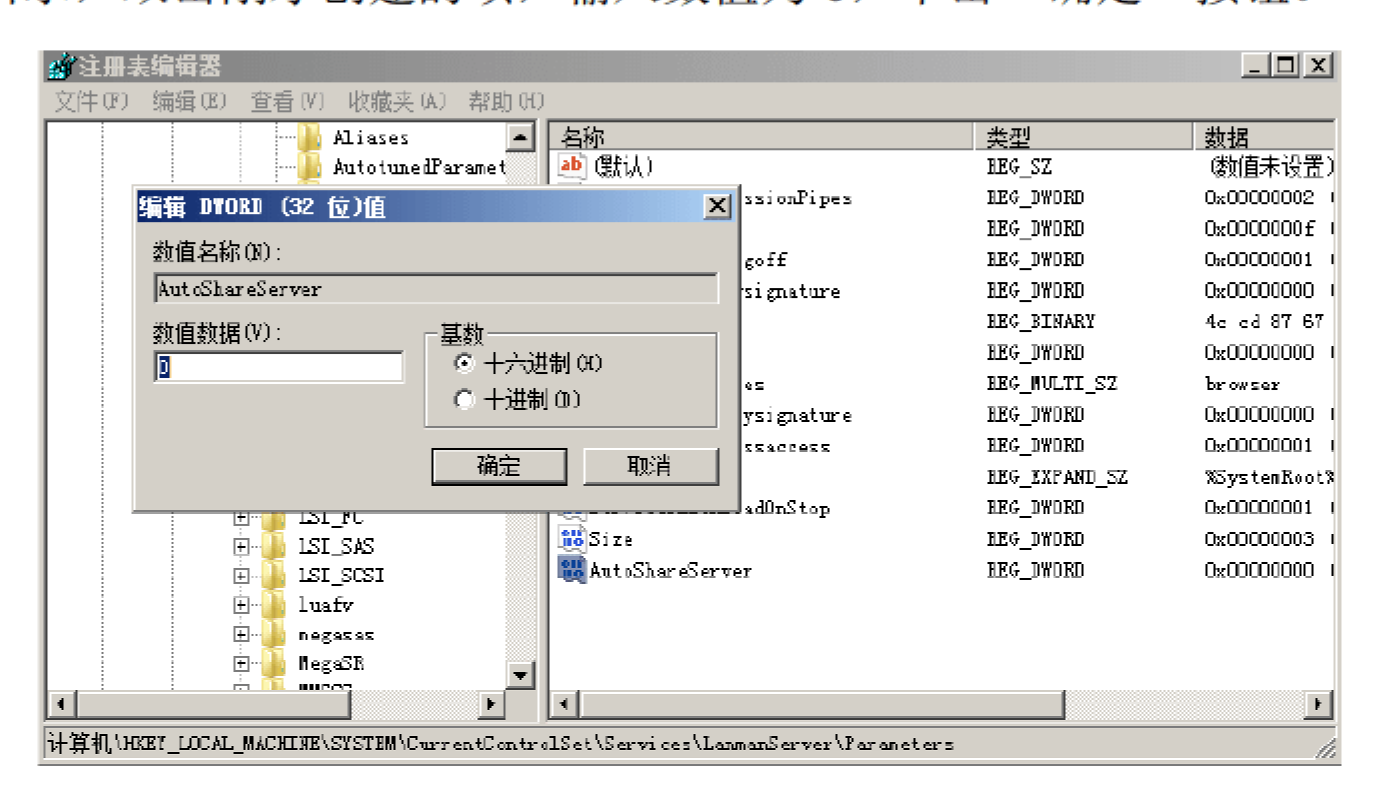


图 7-45　修改键值

④　如果你想禁止 Admin$的默认共享，可以在注册表的以下位置 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters 新建名称：AutoShareWks，类型：REG_DWORD，值：0。

⑤　重启系统。

⑥　如图 7-46 所示，再次查看默认共享已经被禁止。

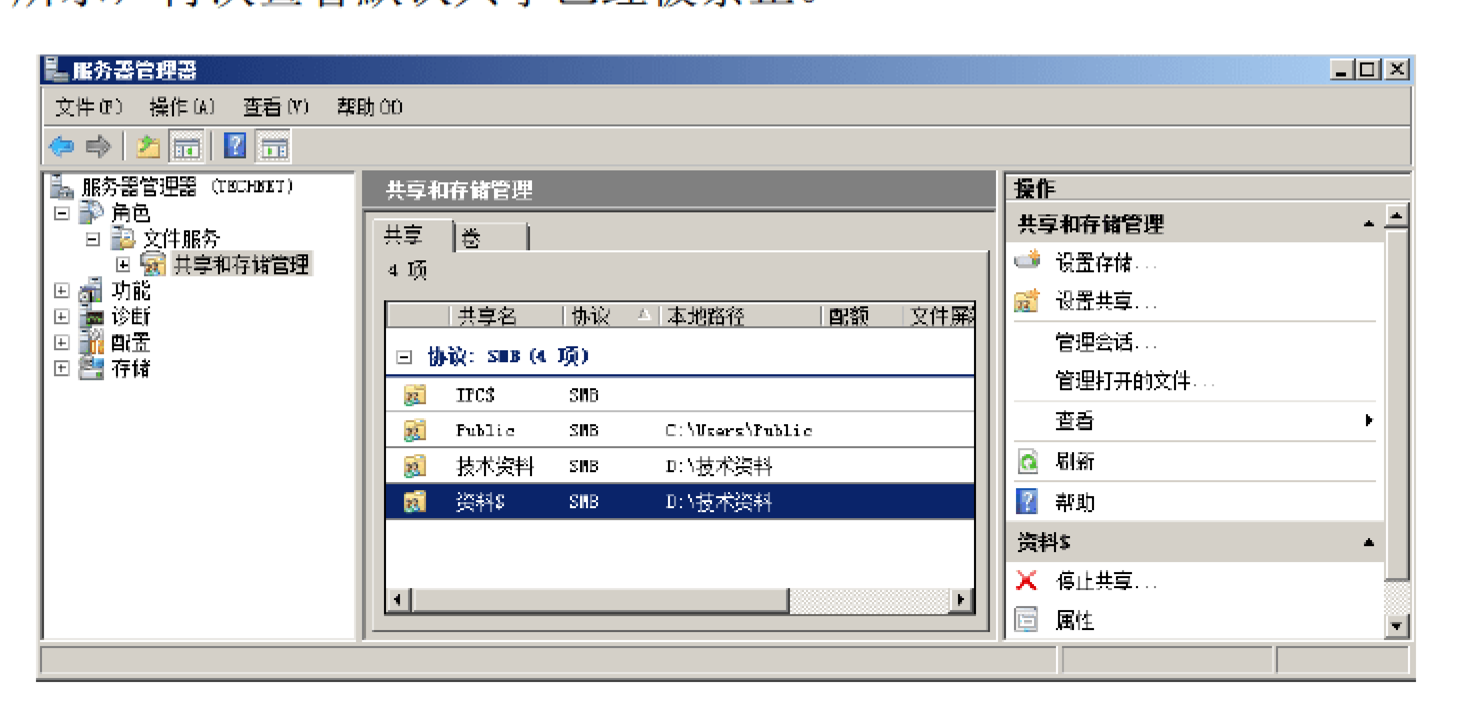


图 7-46　禁止了默认共享

7.3 实战 2：创建基于域的分布式文件系统(DFS)

如果局域网中有多台服务器，并且共享文件夹也分布在不同的服务器上，这就不利于管理员的管理和用户的访问。而使用分布式文件系统，系统管理员就可以把不同服务器上的共享文件夹组织在一起，构建成一个目录树。这在用户看来，所有共享文件仅存储在一个地点，只需访问一个共享的 DFS 根目录，就能够访问分布在网络上的共享文件或文件夹，而不必知道这些文件的实际物理位置。

1. DFS 复制

DFS 复制是一种有效的多主机复制引擎，可用于保持跨有限带宽网络连接的服务器之间的文件夹同步。它将文件复制服务 (FRS) 替换为用于 DFS 命名空间以及用于复制使用 Windows Server 2008 域功能级别的域中的 Active Directory 域服务 (AD DS) SYSVOL 文件夹的复制引擎。

DFS 复制使用一种称为远程差分压缩 (RDC) 的压缩算法。RDC 检测对文件中数据的更改，并使 DFS 复制仅复制已更改的文件块而非整个文件。

若要使用 DFS 复制，必须创建复制组并将已复制文件夹添加到组。复制组、已复制文件夹和成员的关系在图 7-47 中进行了说明。

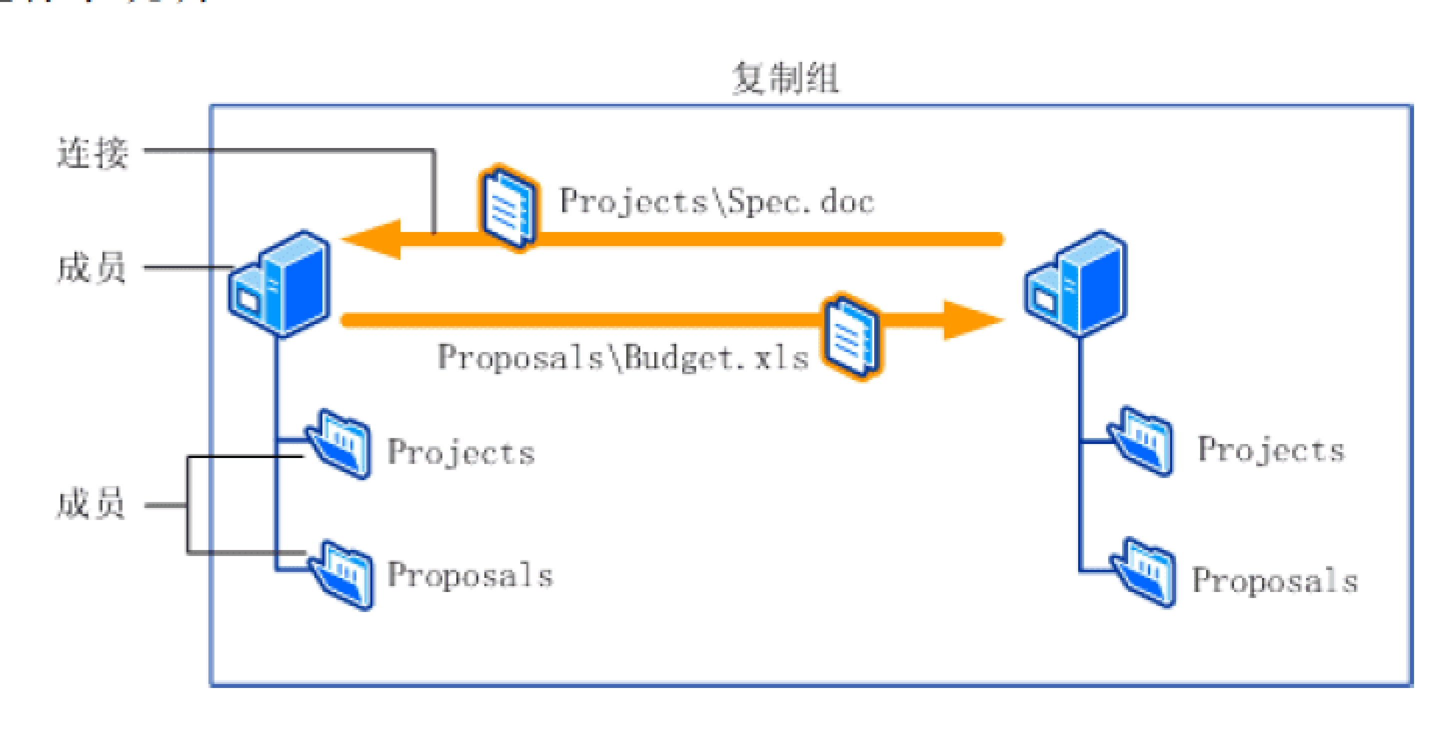


图 7-47 复制组

此图所示复制组是一组称为“成员”的服务器，它参与一个或多个已复制文件夹的复制。“已复制文件夹”是在每个成员上保持同步的文件夹。图中有两个已复制文件夹：Projects 和 Proposals。每个已复制文件夹中的数据更改时，将通过复制组成员之间的连接复制更改。所有成员之间的连接构成复制拓扑。

如果在一个复制组中创建多个已复制文件夹，可以简化部署已复制文件夹的过程，因为该复制组的拓扑、计划和带宽限制将应用于每个已复制文件夹。若要部署其他已复制文件夹，可以使用 Dfsradmin.exe 或按照向导中的说明来定义新的已复制文件夹的本地路径和权限。

每个已复制文件夹具有唯一的设置，例如文件和子文件夹筛选器，以便可以为每个已复制文件夹筛选出不同的文件和子文件夹。

存储在每个成员上的已复制文件夹可以位于成员中的不同卷上，已复制文件夹不必是共享文件夹也不必是命名空间的一部分。但是，“DFS 管理”管理单元使得易于共享已复制文件夹，并选择性地在现有命名空间中发布它们。

在两个或更多成员修改文件并且每个成员没有看到其他成员的版本时，“DFS 复制”使用“最后写入

者优先”的方法来确定要保留的文件版本。放弃的文件存储在解决冲突的成员的冲突和已删除文件夹中。冲突和已删除文件夹还可以用于存储从已复制文件夹中删除的文件。每个冲突和已删除文件夹都有配额，用于控制为进行清理而清除文件的时间。

2. 任务描述

DCServer 是 Ess.com 域的域控制器和 DNS 服务器， FileServer 和 ProfileServer 是两个文件服务器，Research 是研发部门的计算机，Sales 是销售部门的计算机。这些计算机都加入了 Ess.com 域。

为了给域用户访问 FileServer 和 ProfileServer 服务器以及在 Research 服务器上共享资源提供方便，将分布在这些服务器上的资源逻辑整合在 DCServer 上创建的一个“常用文件”文件夹中。

为了使 FileServer 服务器上的“安装文件”文件夹容错和负载均衡，将 ProfileServer 的“安装文件”添加到 DCServer 上“常用文件”中的“安装文件”目标上。

DFS 还为有分支办公室的网络环境提供了很好的支持。可以将用户透明地定向到网络连接较好的服务器上。

3. 实战环境

- DCServer 安装了 Windows Server 2008 企业版操作系统。
- FileServer 安装了 Windows Server 2008 企业版操作系统。
- Research 安装了 Windows Server 2008 企业版操作系统。
- ProfileServer 安装 Windows Server 2008 企业版核心。
- Sales 安装了 Vista 操作系统。

如图 7-48 所示，在文件服务器 Research 上有个共享文件夹“技术资料”，在 FileServer 上有共享文件夹“安装文件”。我们在 DCServer 服务器上创建一个共享文件夹“常用文件”，这个“常用文件”就是 DFS 的根，然后添加两个连接指向“安装文件”和“技术资料”两个共享文件，这两个连接在用户看来就像“常用文件”文件夹中的两个子文件夹。用户单击“常用文件”中的“技术资料”文件夹将会把用户透明地定位到\\Research\技术资料。

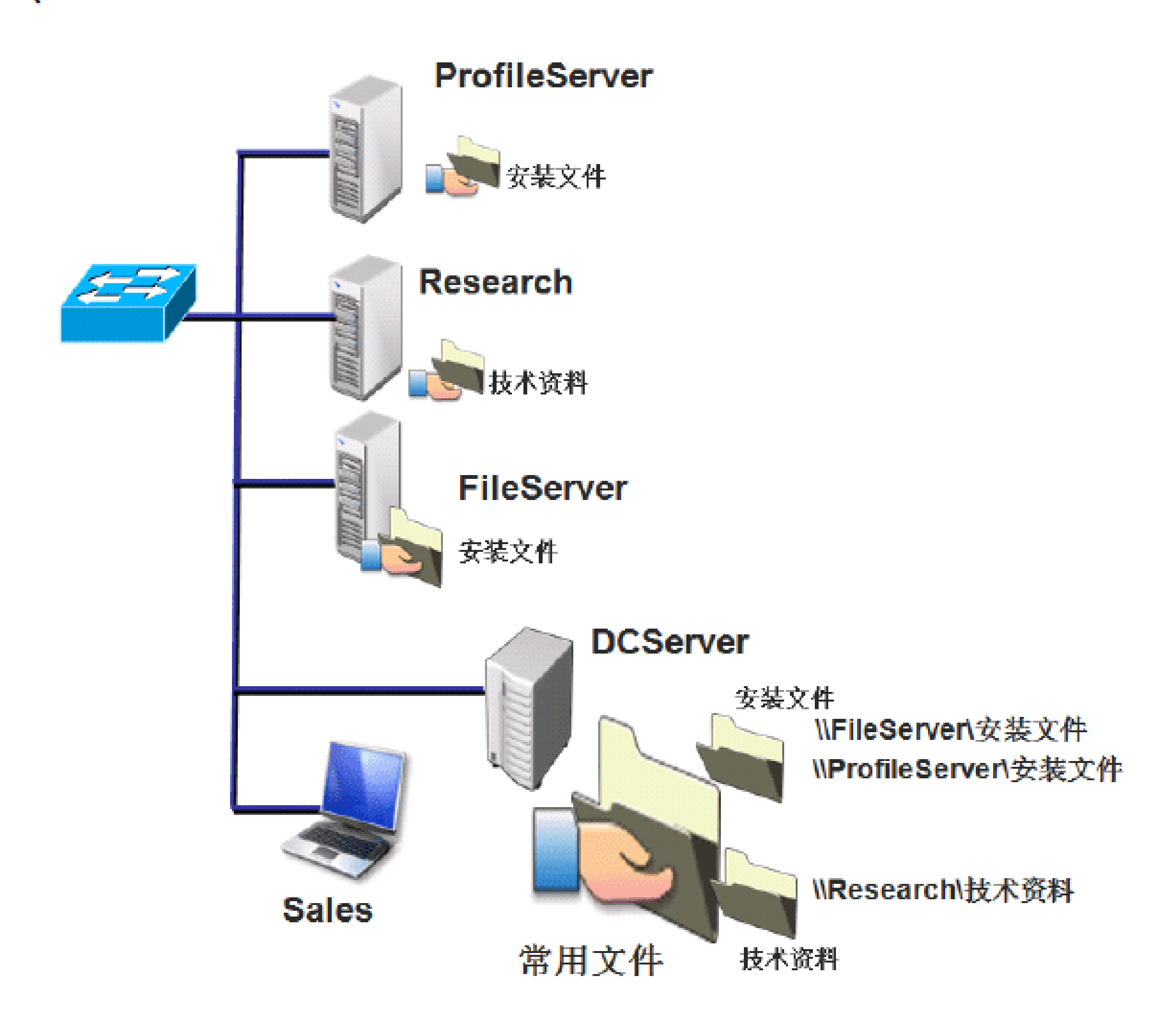


图 7-48 实战环境

在 DCServer 上“常用文件”中的“安装文件”，连接指向了“\\FileServer\安装文件”和“\\ProfileServer\安装文件”两个网络文件夹。这两个文件夹会实现自动同步。大量用户访问“\\DCServer\常用文件\安装文件”时，将会把用户均匀地定位到两个服务器上，从而实现负载均衡。如果其中的 ProfileServer 服务损坏，用户会自动全部定位到 FileServer 服务器上的“安装文件”文件夹，这样实现容错。

4. 实战目标

- 创建基于域的分布式文件系统。
- 访问基于域的分布式文件系统。
- 实现对分支办公室的支持。

7.3.1 任务 1：创建基于域的 DFS

在服务器上安装以下角色。

- 在 FileServer 上安装“分布式文件系统”、“DFS 复制”和“文件服务器”。
- 在 Research 上安装“分布式文件系统”、“DFS 复制”和“文件服务器”。
- 在 DCServer 上安装“DFS 命名空间”，并创建命名空间，在该命名空间中添加文件夹。

创建基于域的 DFS

① 以域管理员用户账户登录 FileServer。

② 打开“服务器管理器”窗口，单击“文件服务”选项，可以看到有些文件服务器角色服务没有安装。

③ 如图 7-49 所示，单击“添加角色”按钮。

④ 如图 7-50 所示，在出现的“选择角色服务”界面中，选中“DFS 命名空间”、“DFS 复制”、“文件复制服务”复选框。

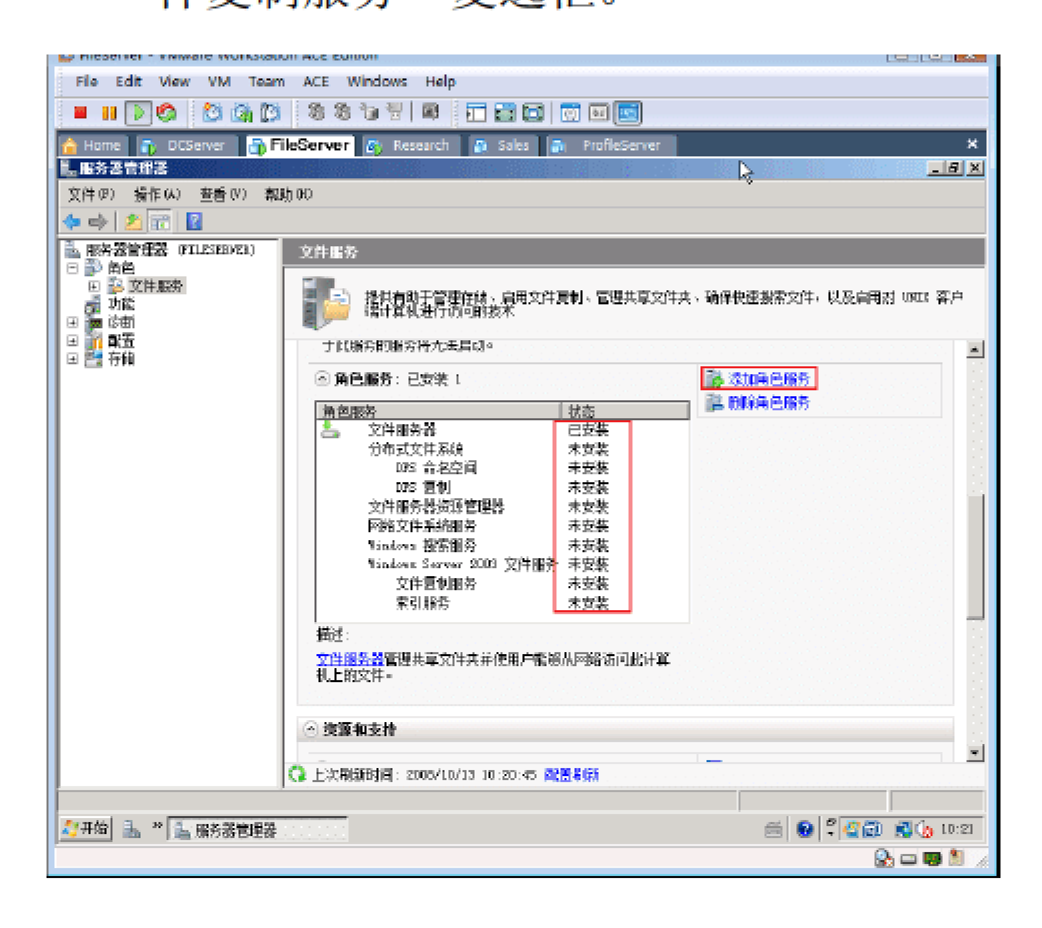


图 7-49　添加角色

图 7-50　选择角色服务

⑤ 如图 7-51 所示，在出现的“配置存储使用情况监视”界面中，单击“下一步”按钮，完成安装。

⑥ 以域管理员用户账户登录到 DCServer。

⑦ 打开“服务器管理器”窗口，如图 7-52 所示，单击“添加角色”按钮。

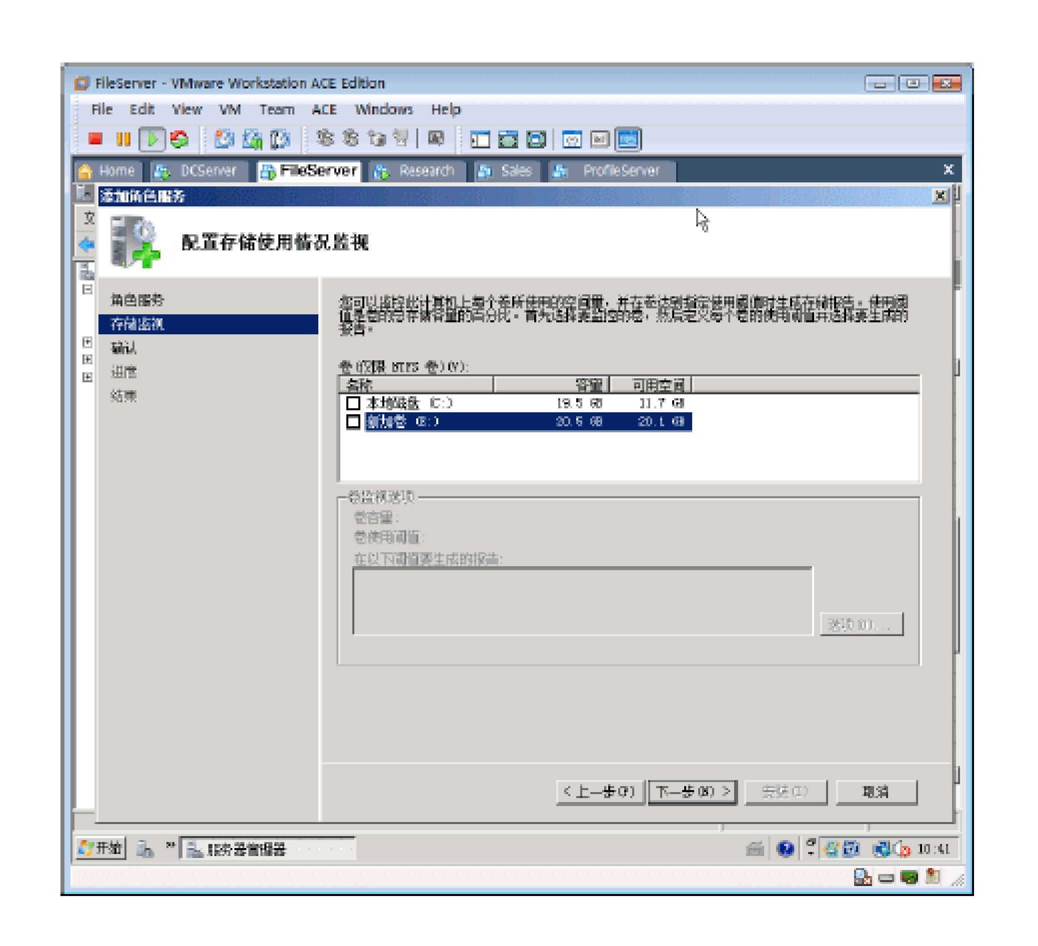


图 7-51　配置存储使用情况监视

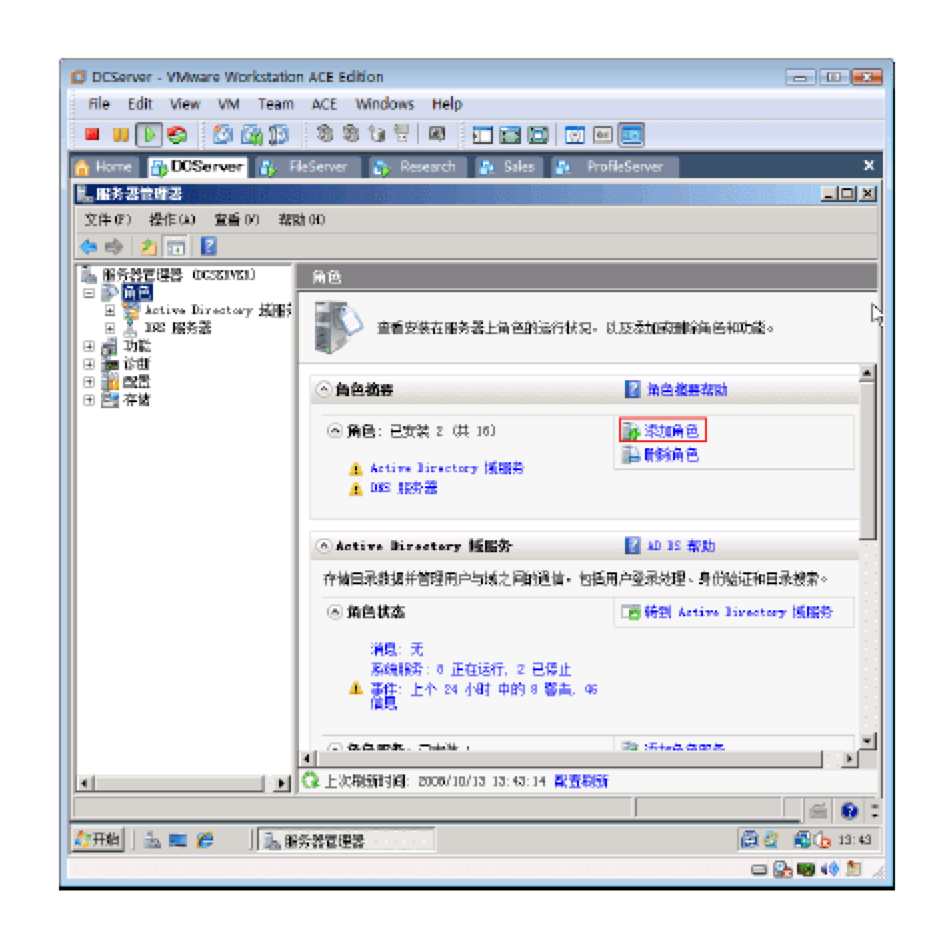


图 7-52　添加角色

⑧ 如图 7-53 所示，在出现的“选择服务器角色”界面中，选中“文件服务”复选框，单击“下一步”按钮。

⑨ 如图 7-54 所示，在出现的“选择角色服务”界面中，选中“FDS 命名空间”复选框，单击“下一步”按钮。

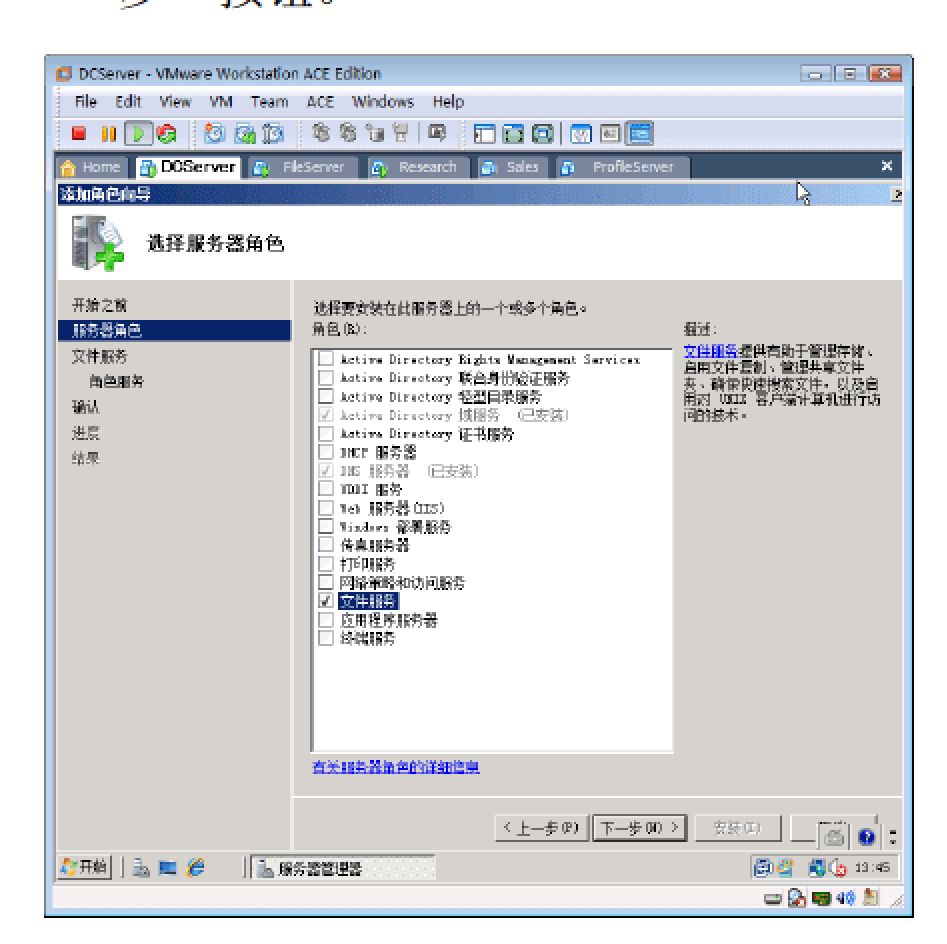


图 7-53　选择角色

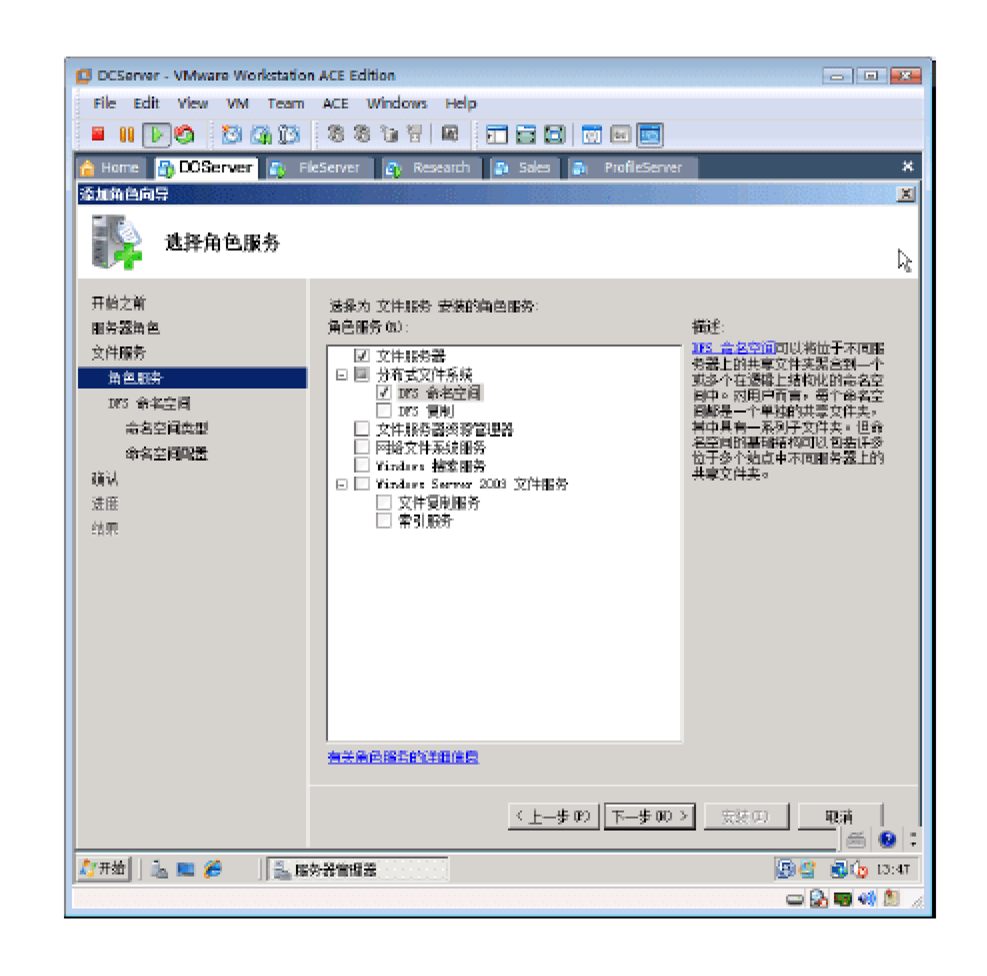


图 7-54　选择角色服务

⑩ 如图 7-55 所示，在出现的“文件服务”界面中，单击“下一步”按钮。

⑪ 如图 7-56 所示，在出现的“创建 DFS 命名空间”界面中，选中“立即使用此向导创建命名空间”单选按钮，在文本框中输入“常用文件”，单击“下一步”按钮。

⑫ 如图 7-57 所示，在“选择命名空间类型”界面中，选中“基于域的命名空间”单选按钮，选中“启用 Windows Server 2008 模式”复选框，单击“下一步”按钮。

⑬ 如图 7-58 所示，在“配置命名空间”界面中，单击“下一步”按钮，完成向导。

⑭ 如图 7-59 所示，展开“服务器管理器”中的“文件服务”→“DFS 管理”→“命名空间”→“\\Ess.com\常用文件”节点，单击“新建文件夹”按钮。

⑮ 如图 7-60 所示，在出现的“添加文件夹目标”对话框中，输入名称“技术资料”及文件夹目标，单击“添加”按钮，输入“\\research\技术资料”，单击“确定”按钮。

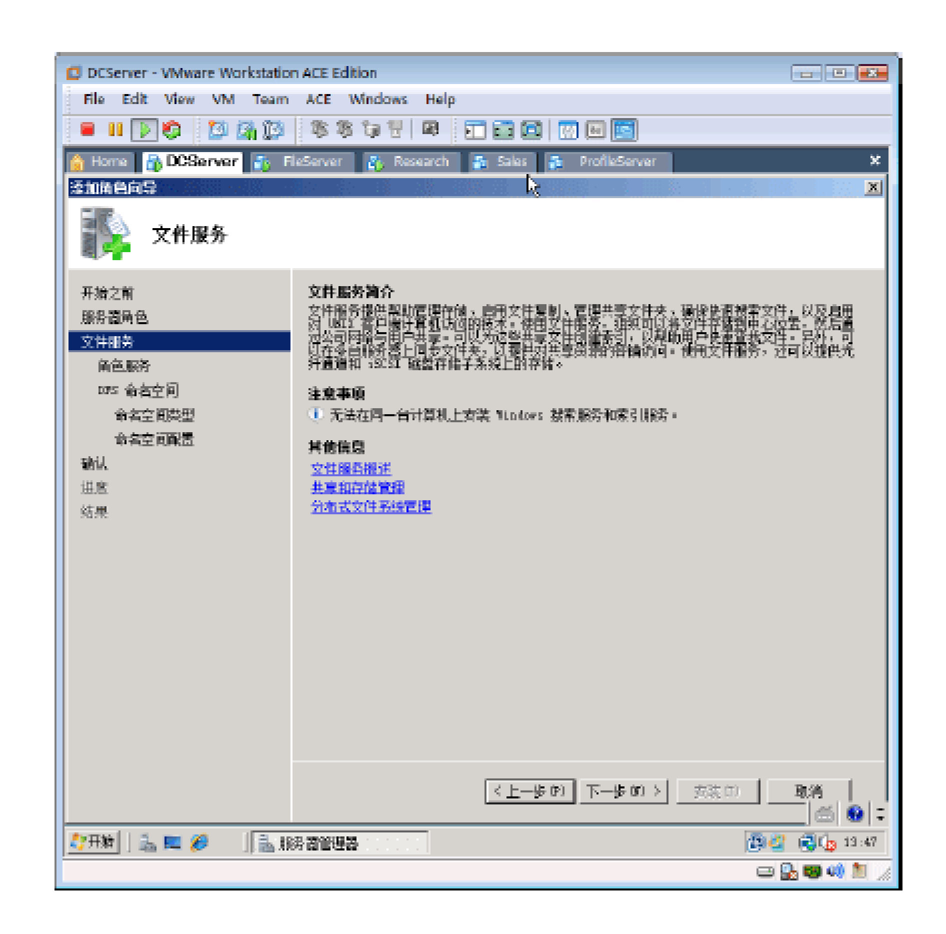


图 7-55　确认文件服务

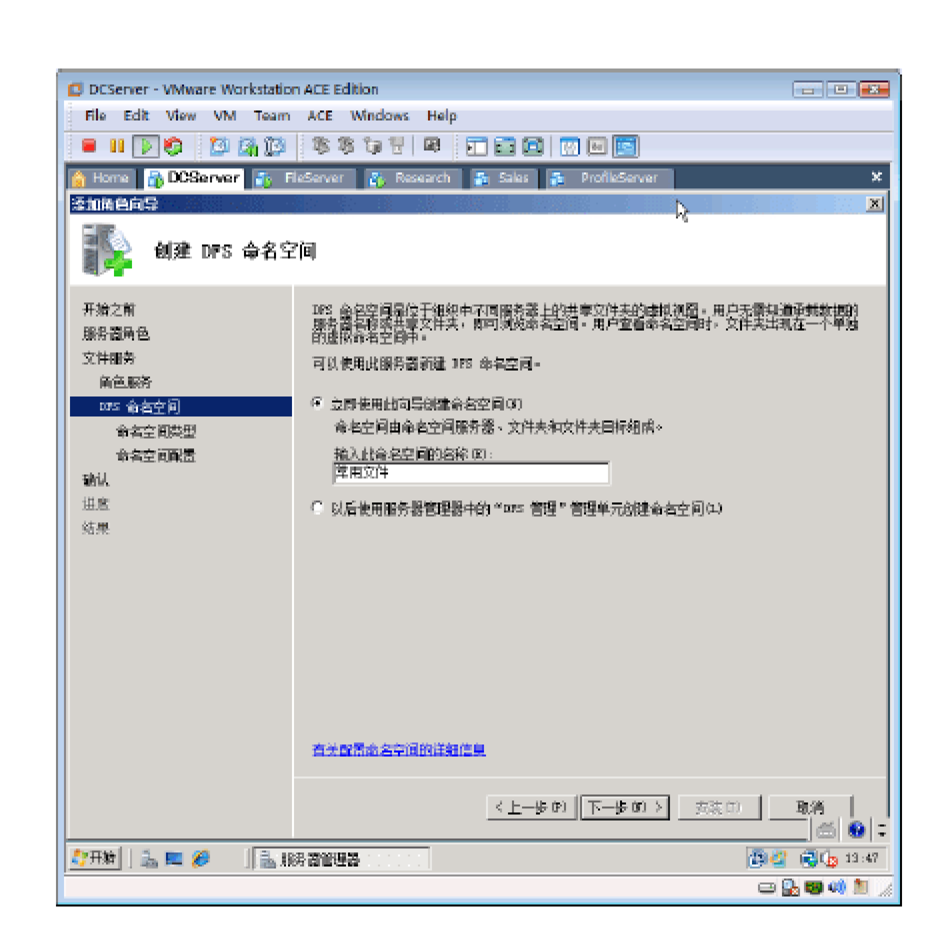


图 7-56　创建 DFS 名称空间

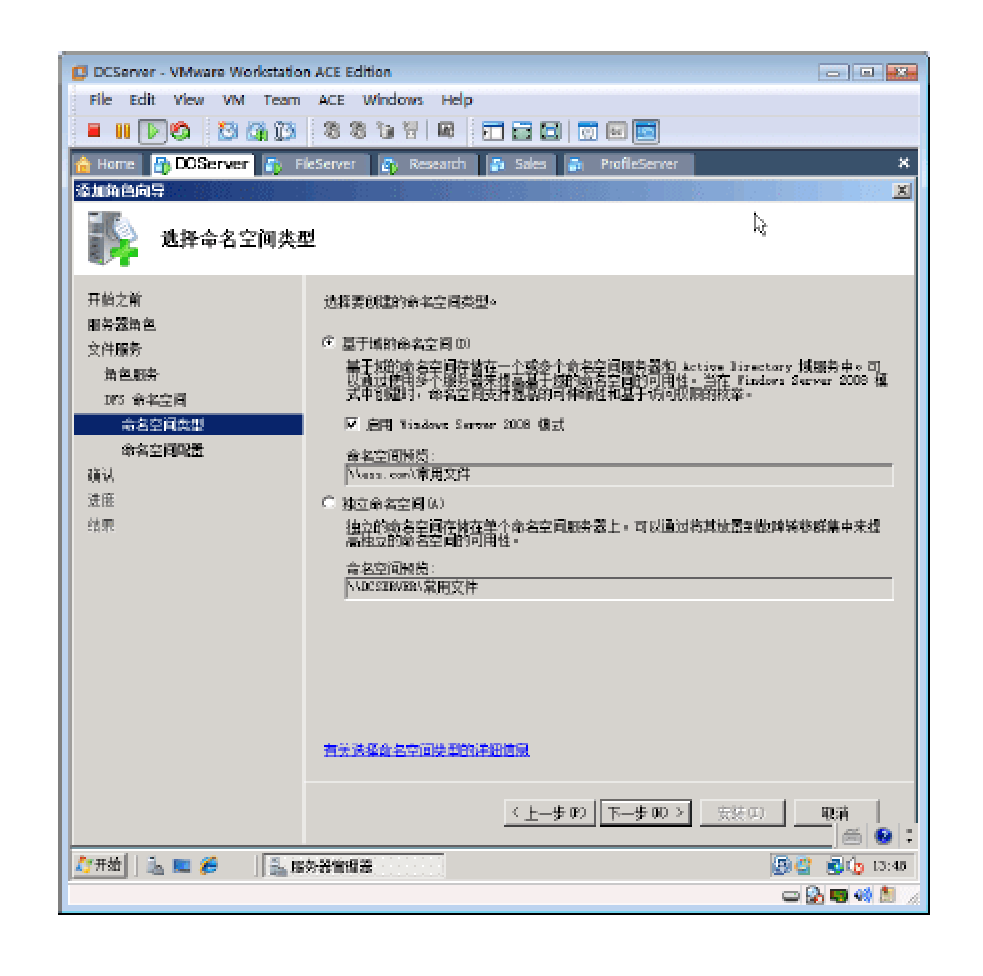


图 7-57　选择名称空间类型

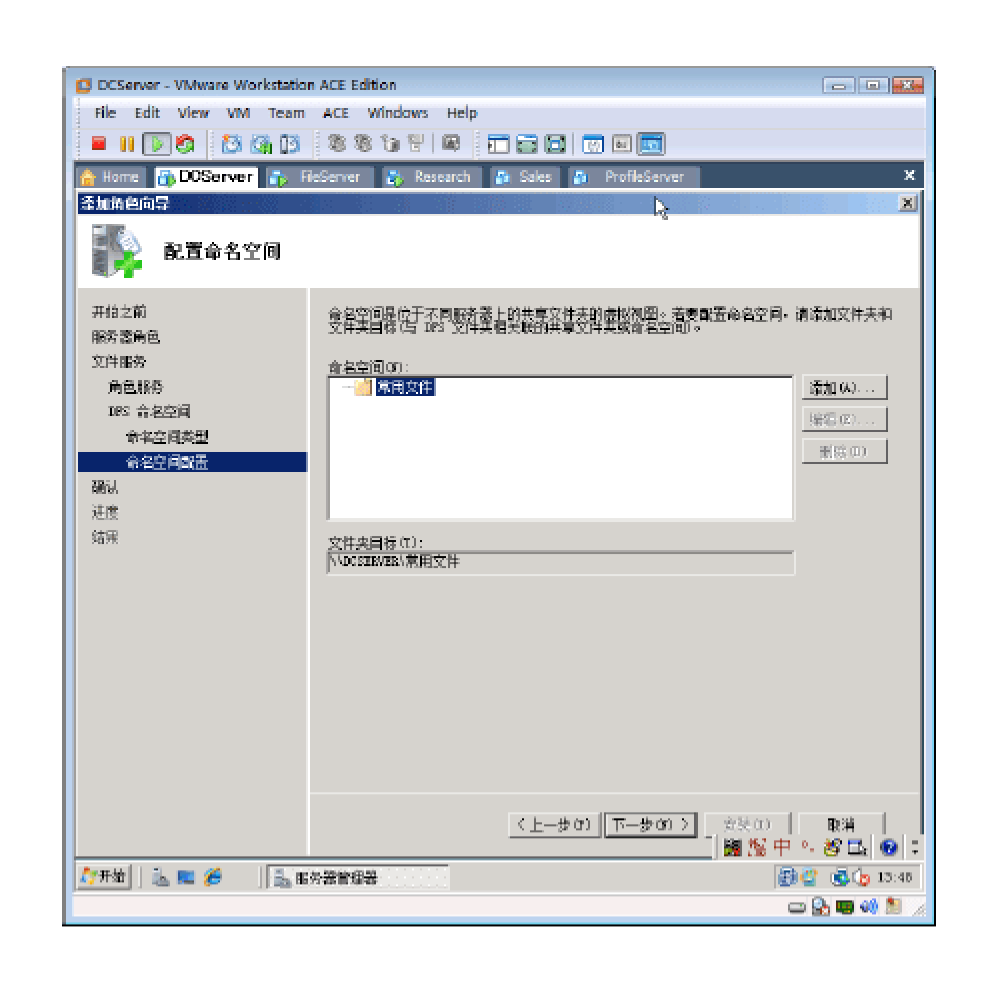


图 7-58　配置名称空间

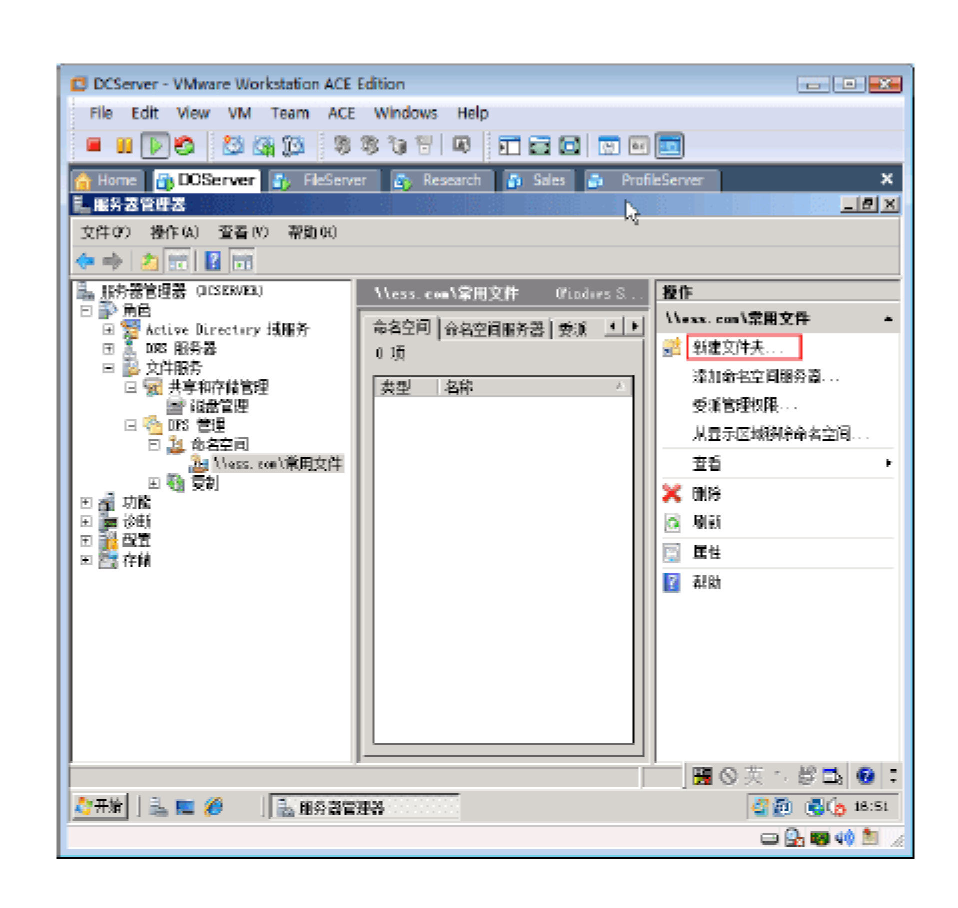


图 7-59　在名称空间中创建文件夹

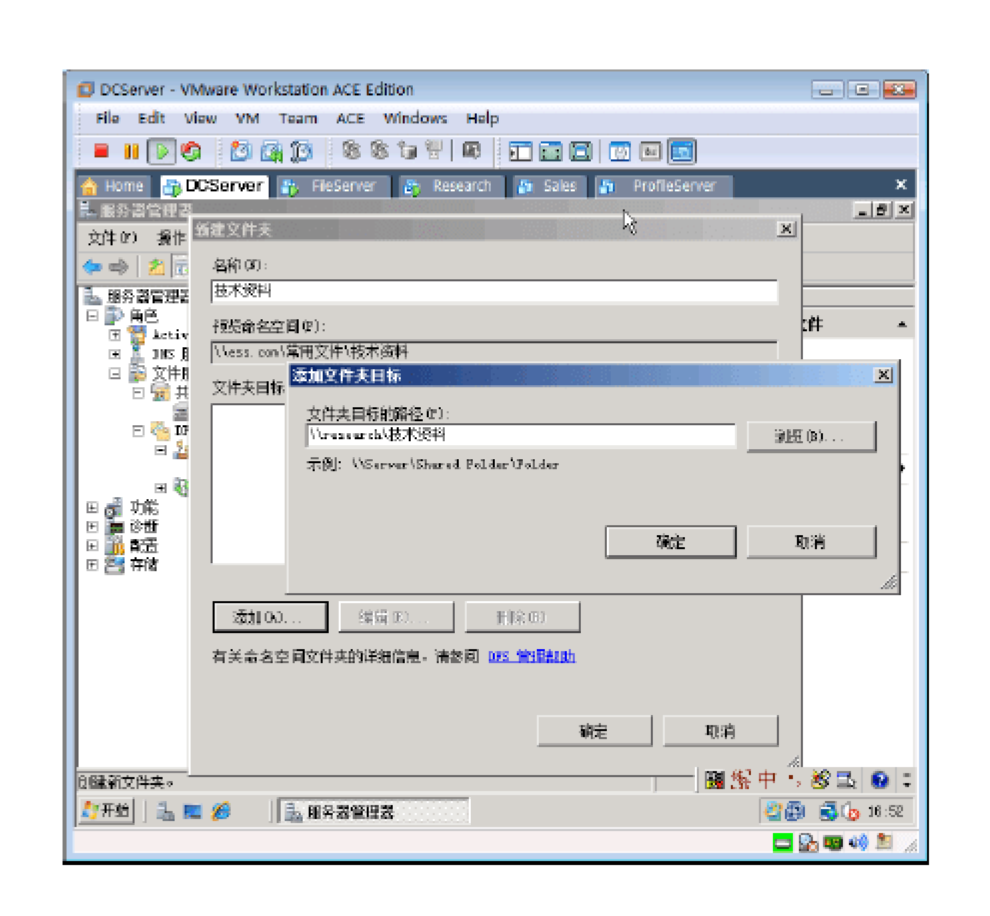


图 7-60　添加目标文件夹

⑯　如图 7-61 所示，单击“确定”按钮，完成新建文件夹。



提示：还可以继续单击“添加”按钮添加多个目标，这些目标文件夹将会自动同步，这样可以避免硬件故障造成的数据丢失，同时多个访问者被均匀地定位到多个目标文件夹，从而实现负载均衡。

⑰ 如图 7-62 所示，使用相同的方法，在该命名空间中，添加指向“\\fileserver\安装文件”的“安装文件”。

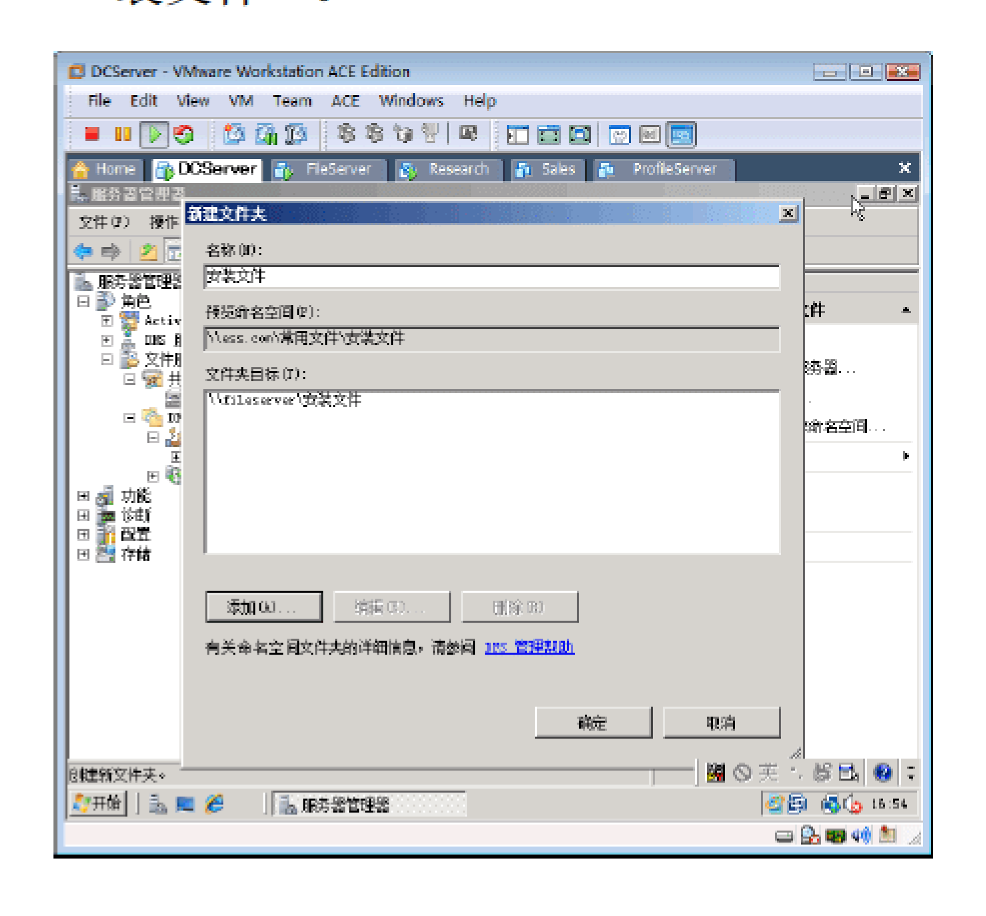


图 7-61　完成添加

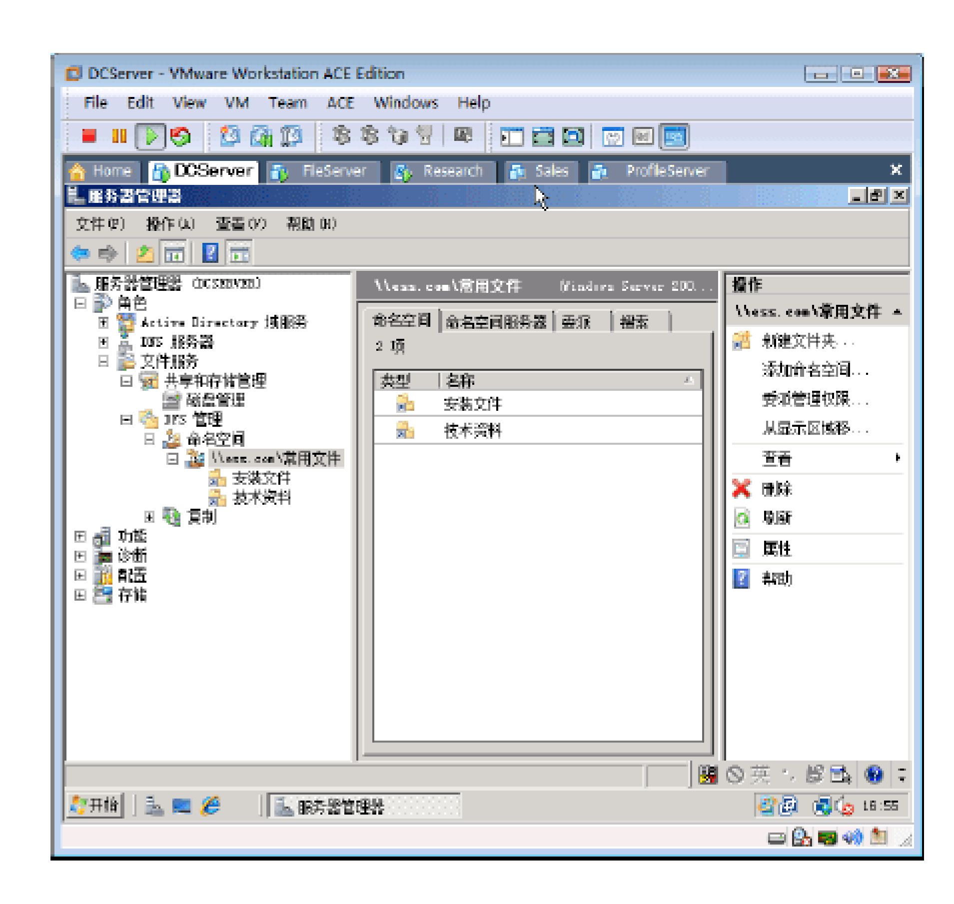


图 7-62　同一个名称空间下的目标文件夹

7.3.2　任务 2：添加多个名称空间

在一个域中可以有多个命名空间，用户也可以使用 DFS 管理工具管理 DFS 命名空间。以下示例演示，在域中创建一个“人力资源”的名称空间。名称空间服务器仍然是 DCServer。这样你就可以在“人力资源”命名空间，组织人力资源相关的文件夹了。

① 选择“开始”→“程序”→“管理工具”→DFS Management 命令。

② 如图 7-63 所示，在出现的“DFS 管理”窗口中，单击“新建命名空间”按钮。

③ 如图 7-64 所示，在出现的“命名空间服务器”界面中，输入 DCServer，单击“下一步”按钮。

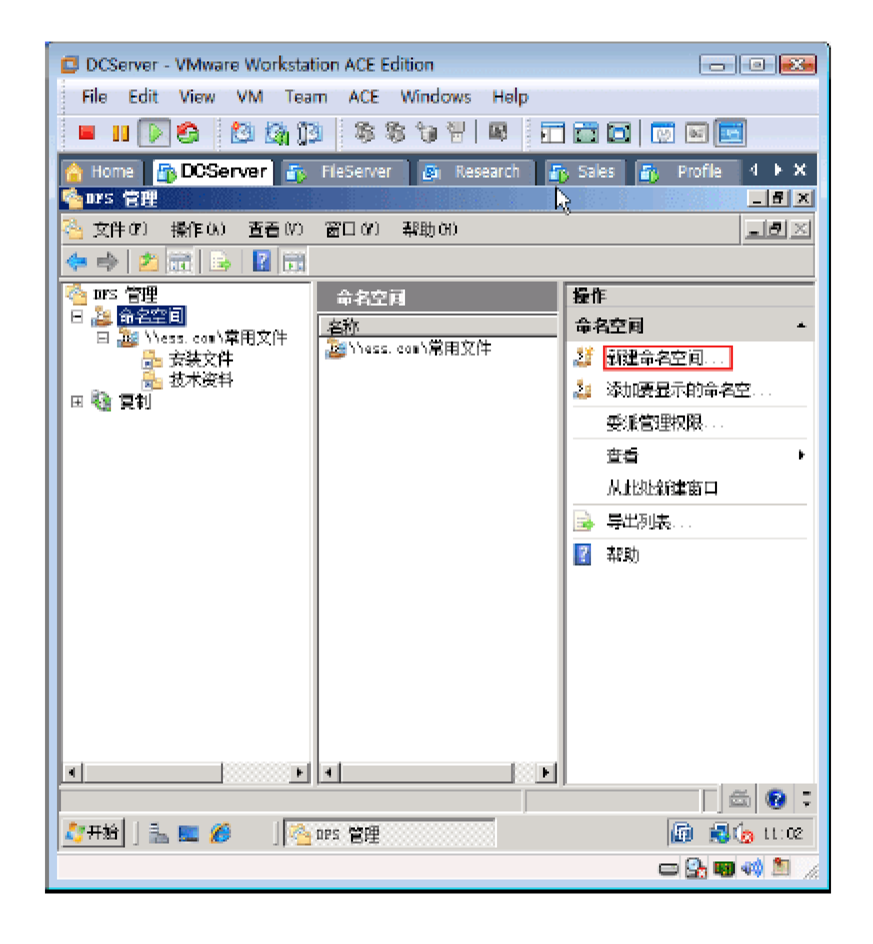


图 7-63　创建新的命名空间

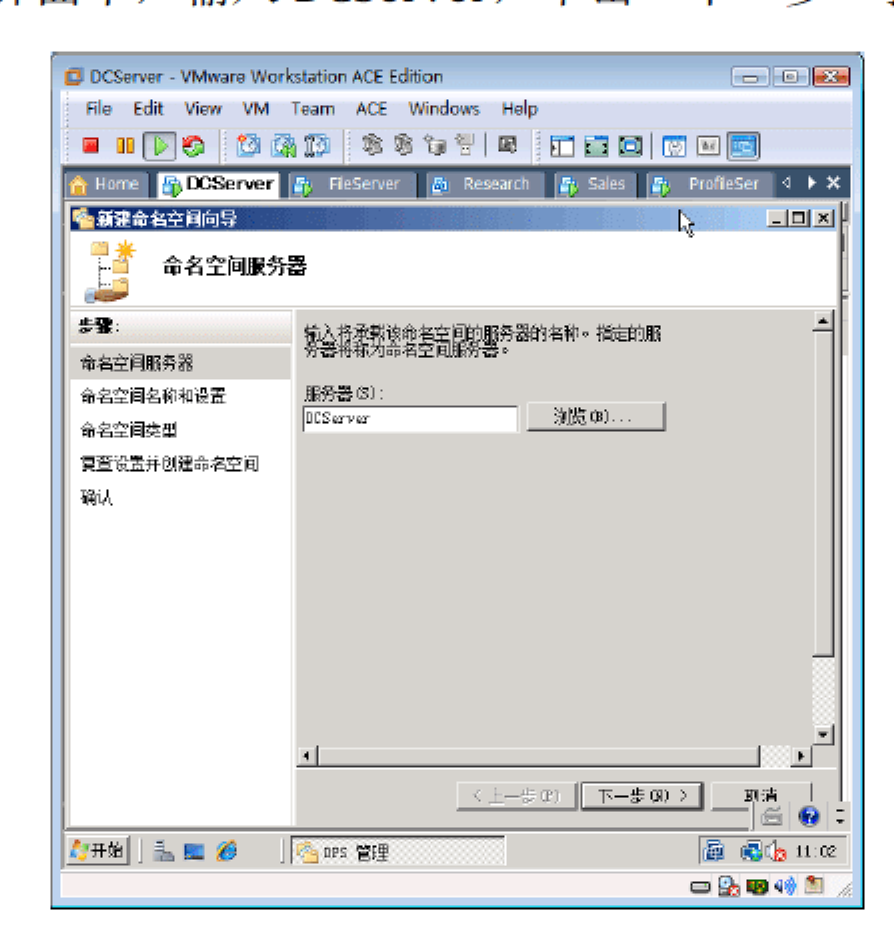


图 7-64　指定命名空间服务器

④ 如图 7-65 所示，在“命名空间名称和设置”对话框中，输入名称“人力资源”，单击“下一步”按钮。

⑤ 如图 7-66 所示，在“命名空间类型”界面中，选中“基于域的命名空间”单选按钮，选中“启用 Windows Server 2008 模式”复选框，单击“下一步”按钮。

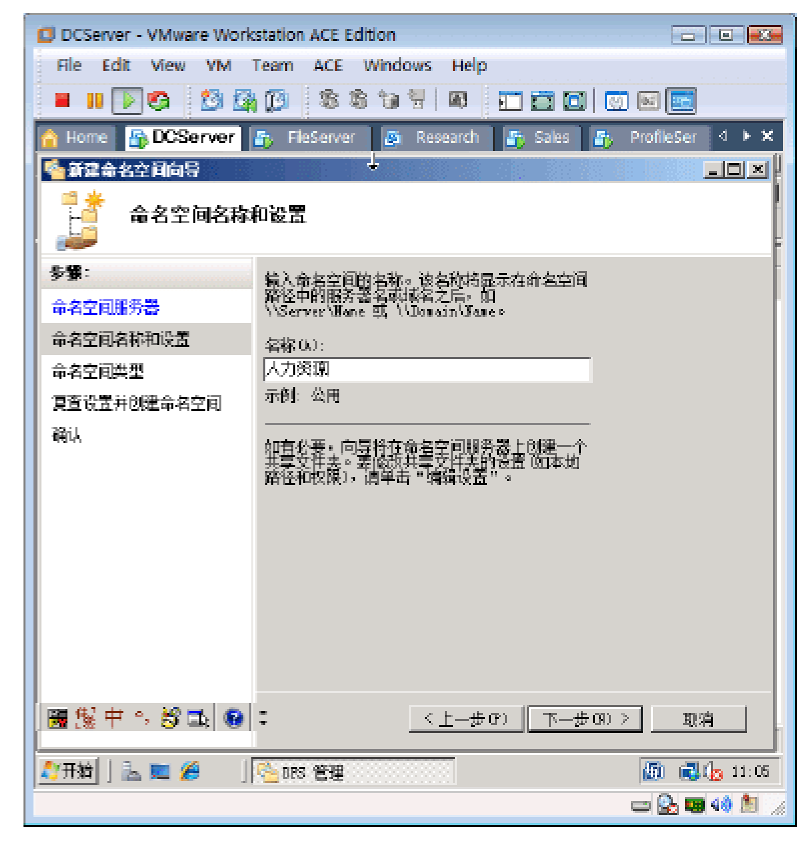



图 7-65　指定命名空间的名称和设置

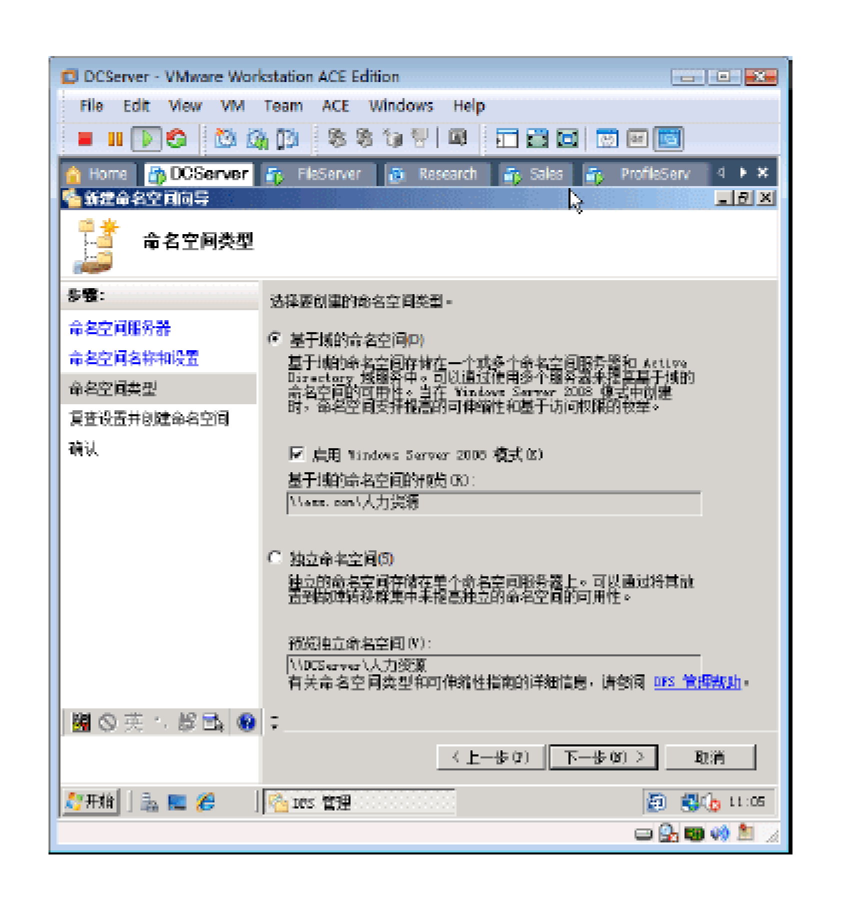


图 7-66　指定命名空间类型

⑥ 如图 7-67 所示，在“复查设置并创建命名空间”界面中，注意观察“命名空间名称\\ess.com\人力资源”，单击“创建”按钮。

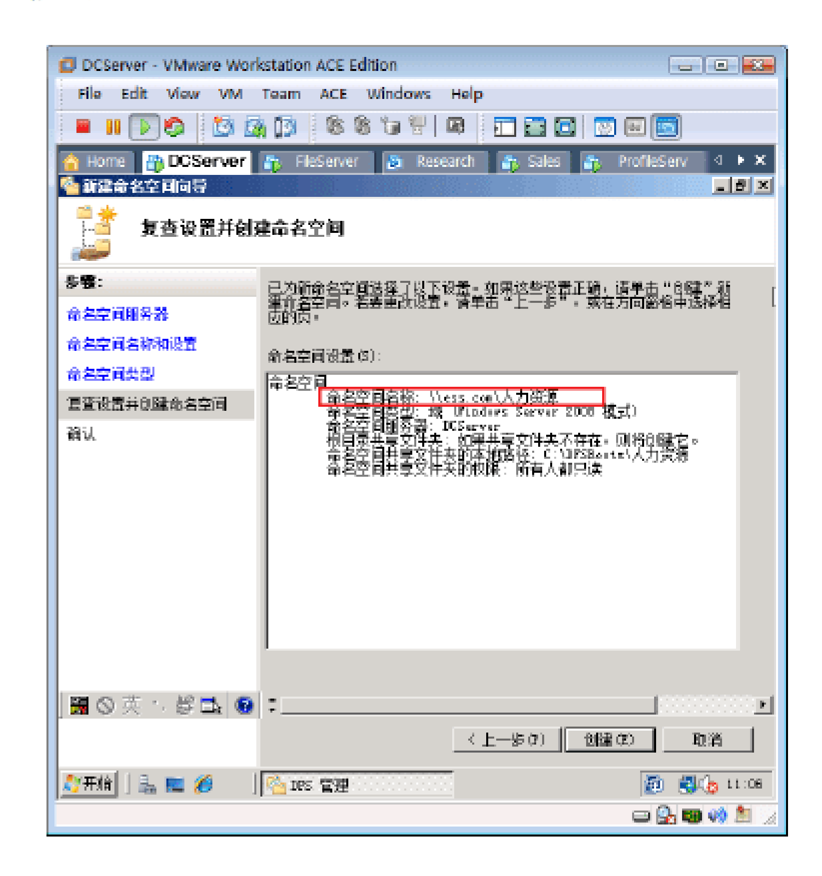


图 7-67　完成命名空间的创建

7.3.3　任务 3：访问命名空间中的文件夹

① 使用域用户账户 Administrator 在 Sales 计算机登录。

② 选择“开始”→“运行”命令，在“运行”对话框中输入\\ess.com，如图 7-68 所示。单击“确定”按钮。



提示：使用命名空间访问共享文件夹，可以看到 ess.com 域中所有的命令空间，如图 7-69 所示。

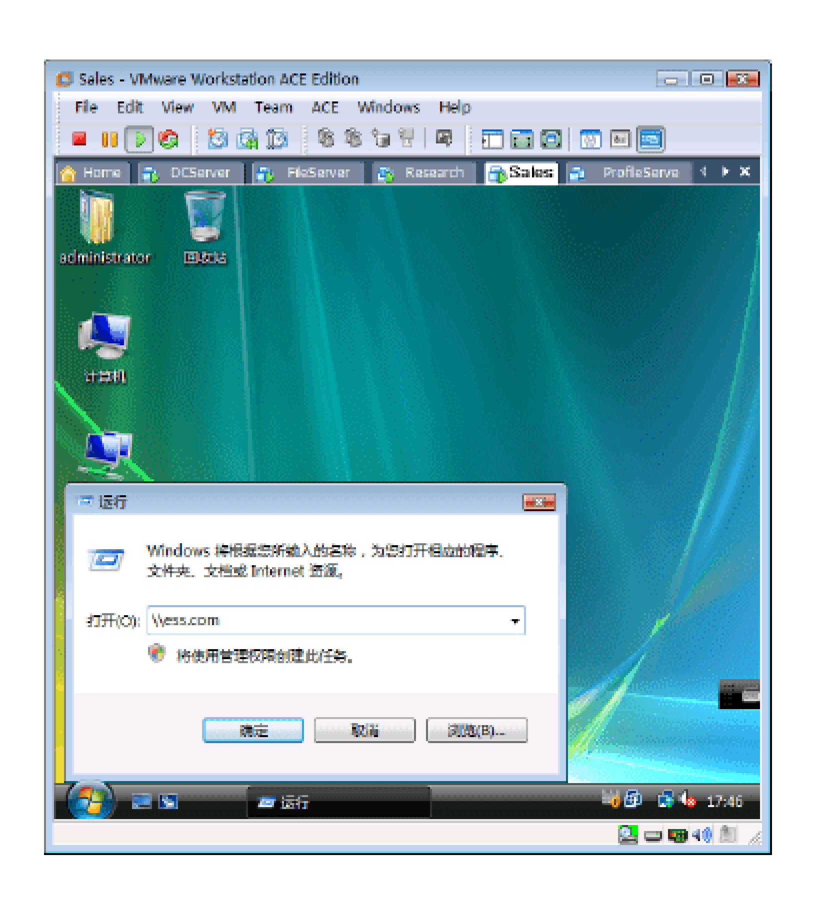


图 7-68　访问命名空间

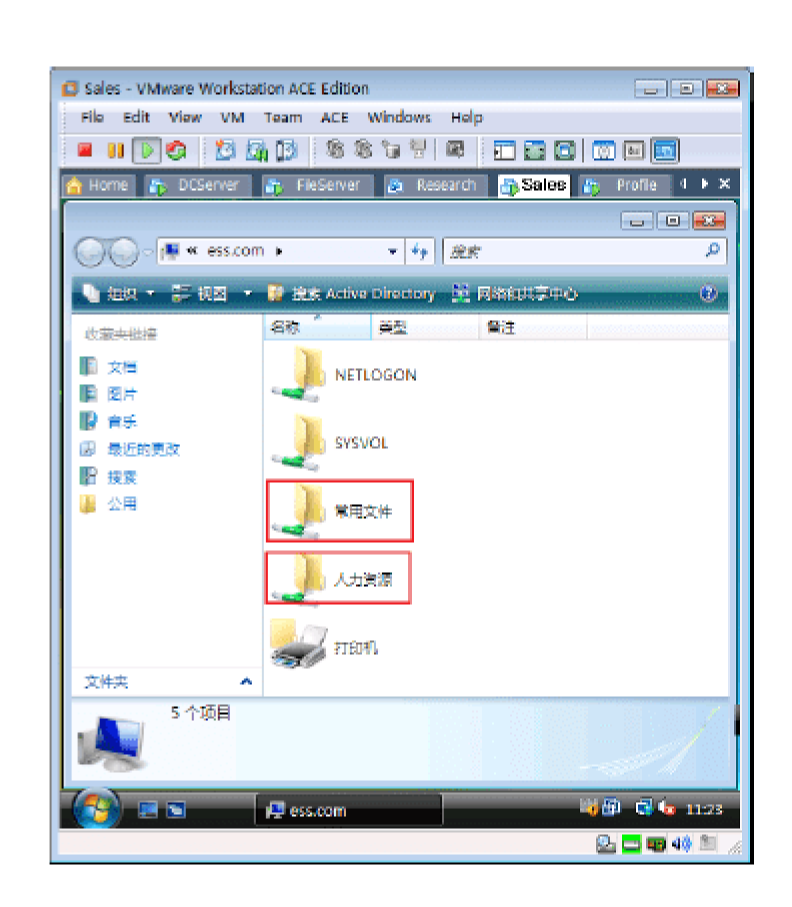


图 7-69　可以看到域中所有的命名空间

③　如图 7-70 所示，单击“常用文件”文件夹，可以看到该名称空间下的两个子文件夹。

④　如图 7-71 所示，双击“安装文件”文件夹，将被透明地定位到“\\FileServer\安装文件”文件夹。

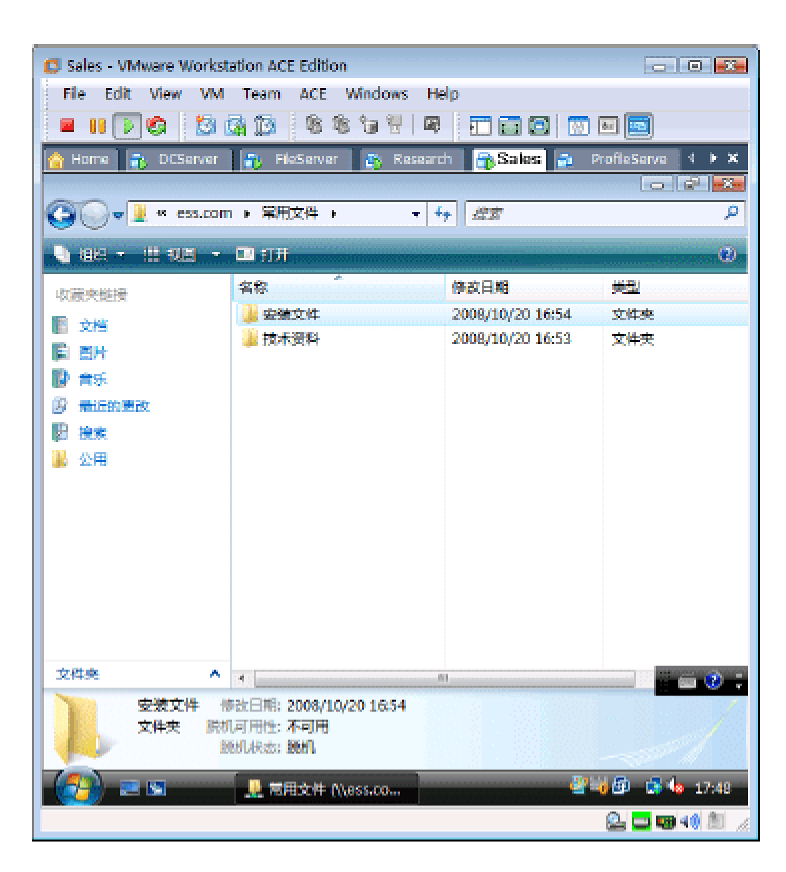


图 7-70　访问名称空间中的文件

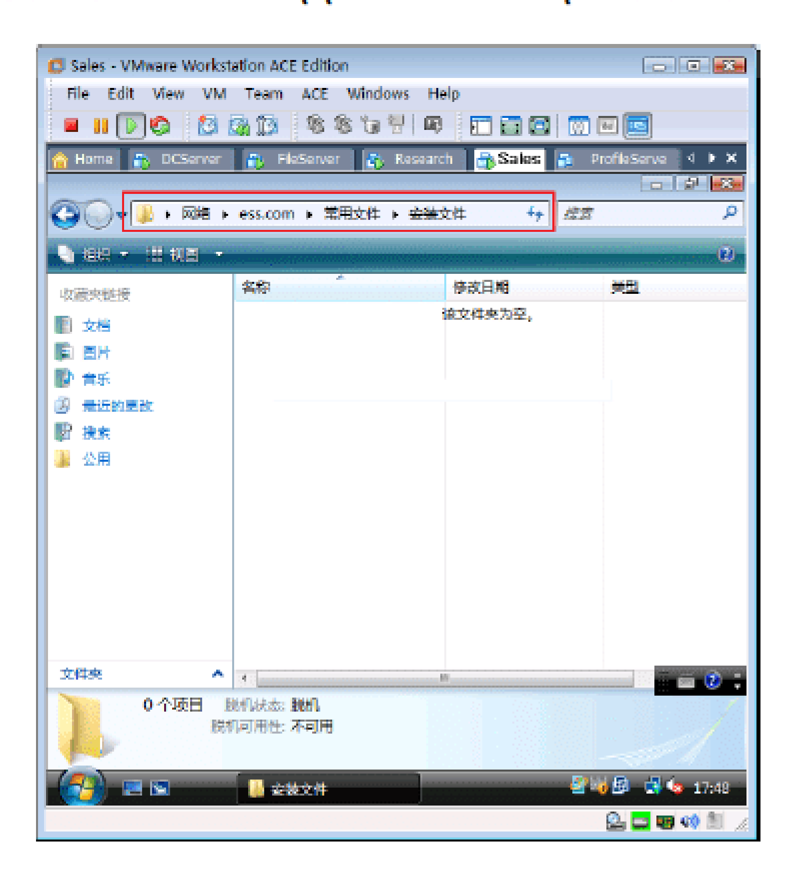


图 7-71　注意访问的路径

⑤　如图 7-72 和图 7-73 所示，也可以直接利用命名空间服务，访问共享资源。

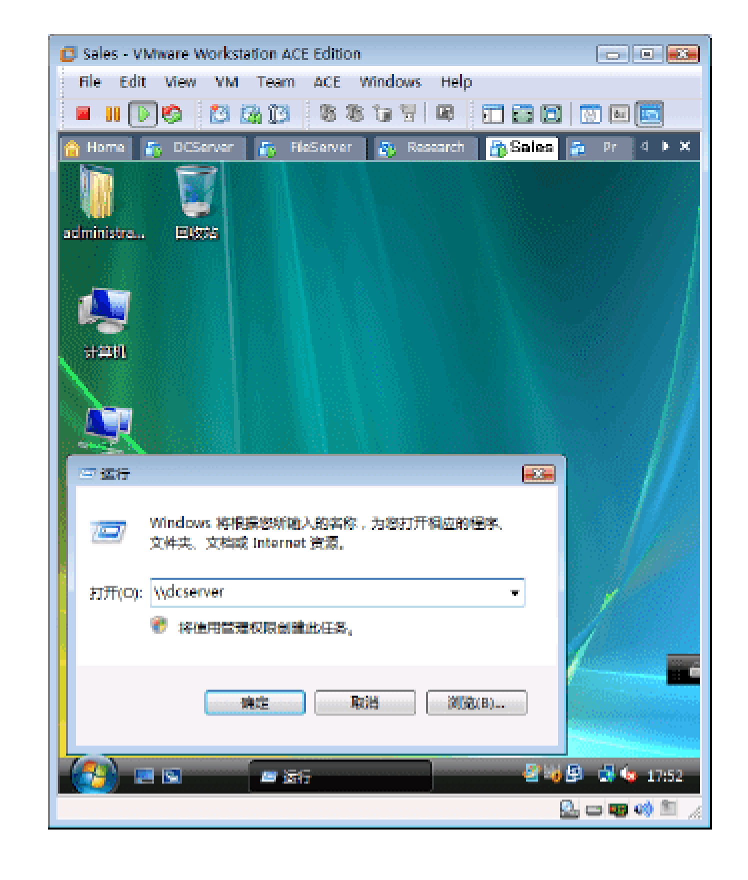


图 7-72　访问命名空间服务器

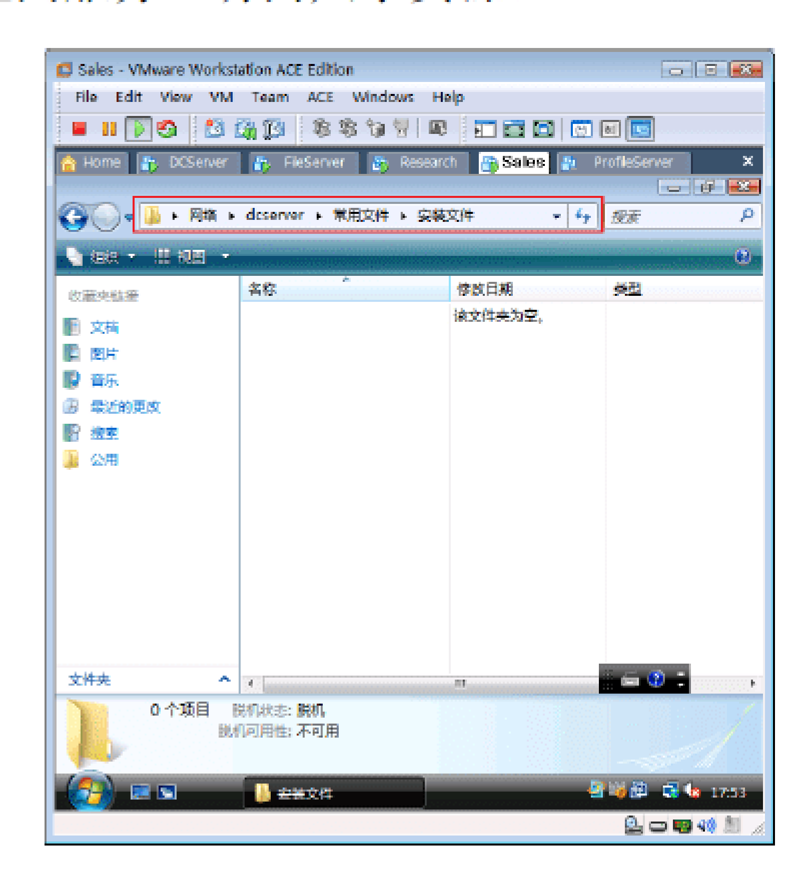


图 7-73　可以访问命名空间中的文件

7.3.4 任务 4：在 Server Core 计算机上添加 DFS 冗余

在 ProfileServer 计算机上安装以下服务。

- 文件复制服务(FRS-Infrastructure)。
- 分布式文件系统服务(DFSN-Server)。
- 分布式文件系统复制(DFSR-Infrastructure-ServerEdition)。

在 DCSever 上添加“安装文件”的冗余文件夹

① 以域管理员的用户账户登录 ProfileServer 计算机。

② 如图 7-74 所示，定位到 C:\windows\system32 目录下，输入 cscript scregedit.wsf /cli 命令显示可用的命令汇总。

③ 如图 7-75 所示，输入 Oclist 命令，显示该计算机安装的和未安装的角色和服务。

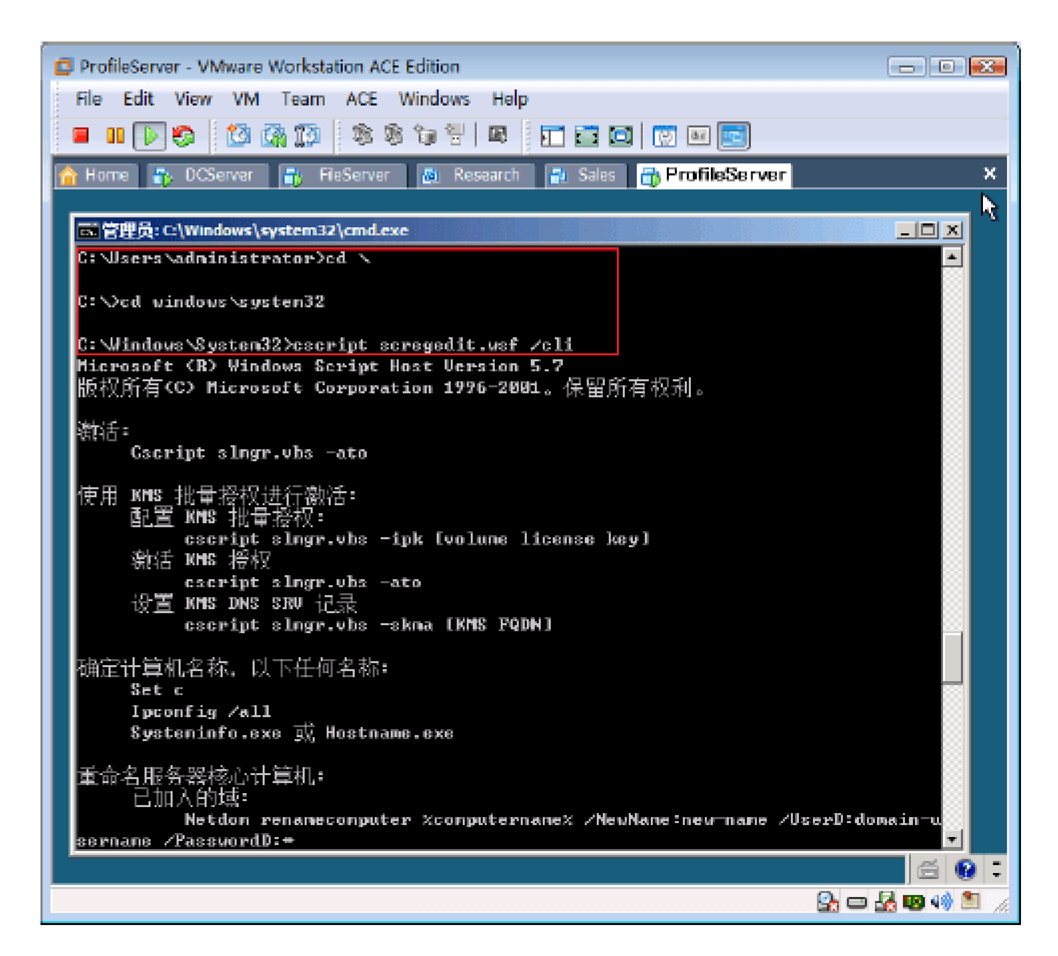


图 7-74 显示命令汇总

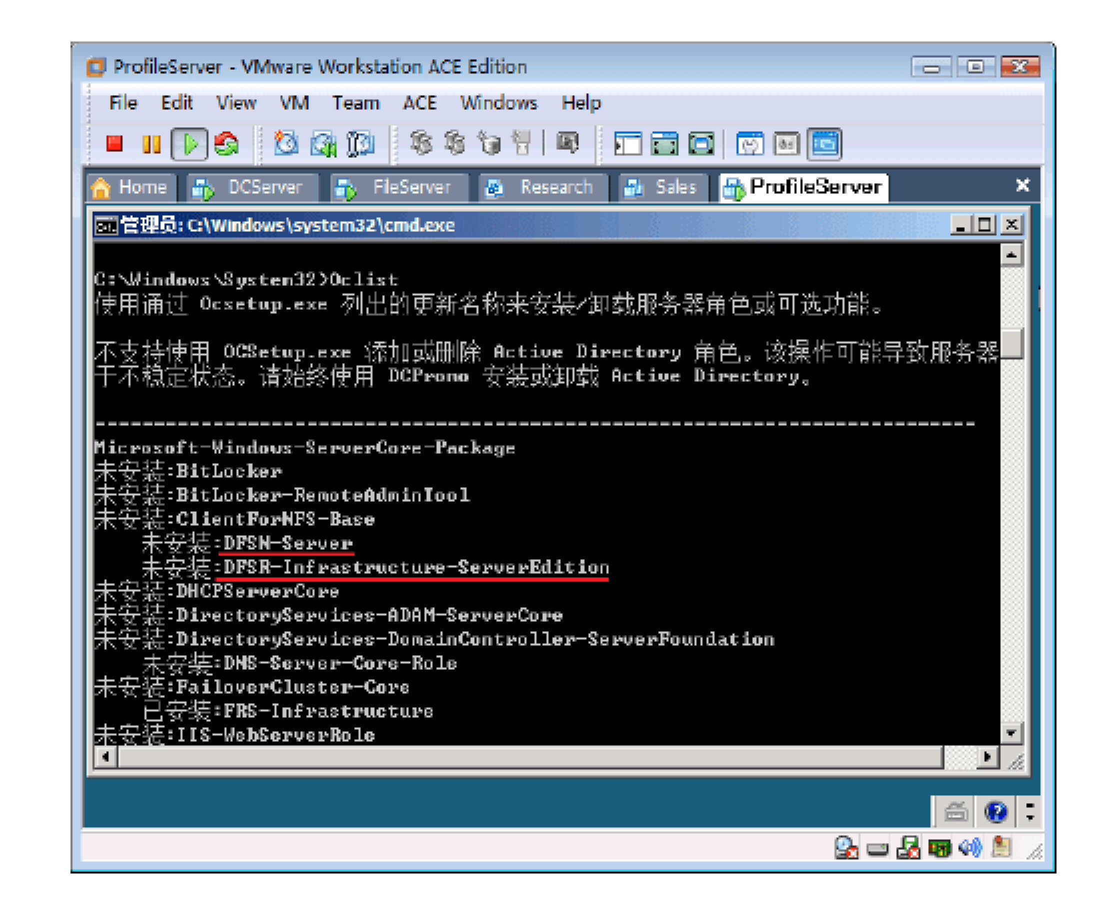


图 7-75 查看安装和未安装的角色和服务

④ 如图 7-76 所示，输入 Start/w Ocsetup FRS-Infrastructure，按 Enter 键。

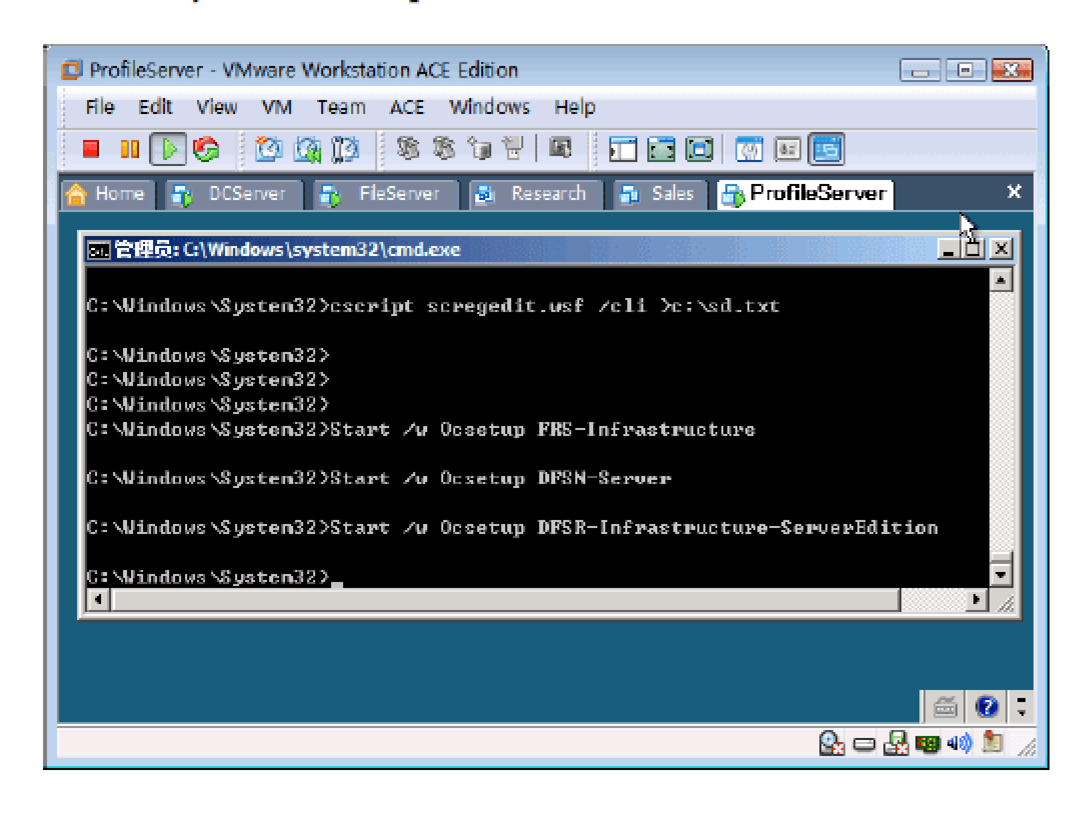
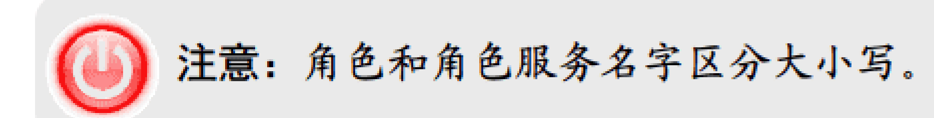


图 7-76 安装角色和角色服务

⑤ 输入 Start/w Ocsetup DFSN-Server，按 Enter 键。

⑥　输入 Start/w Ocsetup DFSR-Infrastructure-ServerEdition，按 Enter 键。



注意：角色和角色服务名字区分大小写。

⑦　以域管理员的用户账户登录到 DCServer。

⑧　选择“开始”→“程序”→“管理工具”→DFS Management 命令。

⑨　在“DFS 管理”对话框，如图 7-77 所示，展开“DFS 管理”→“命名空间”→“安装文件”→“\\ess.com\人力资源”节点，单击“添加文件夹目标”按钮。

⑩　如图 7-78 所示，在出现的“新建文件夹目标”对话框中，单击“浏览”按钮。

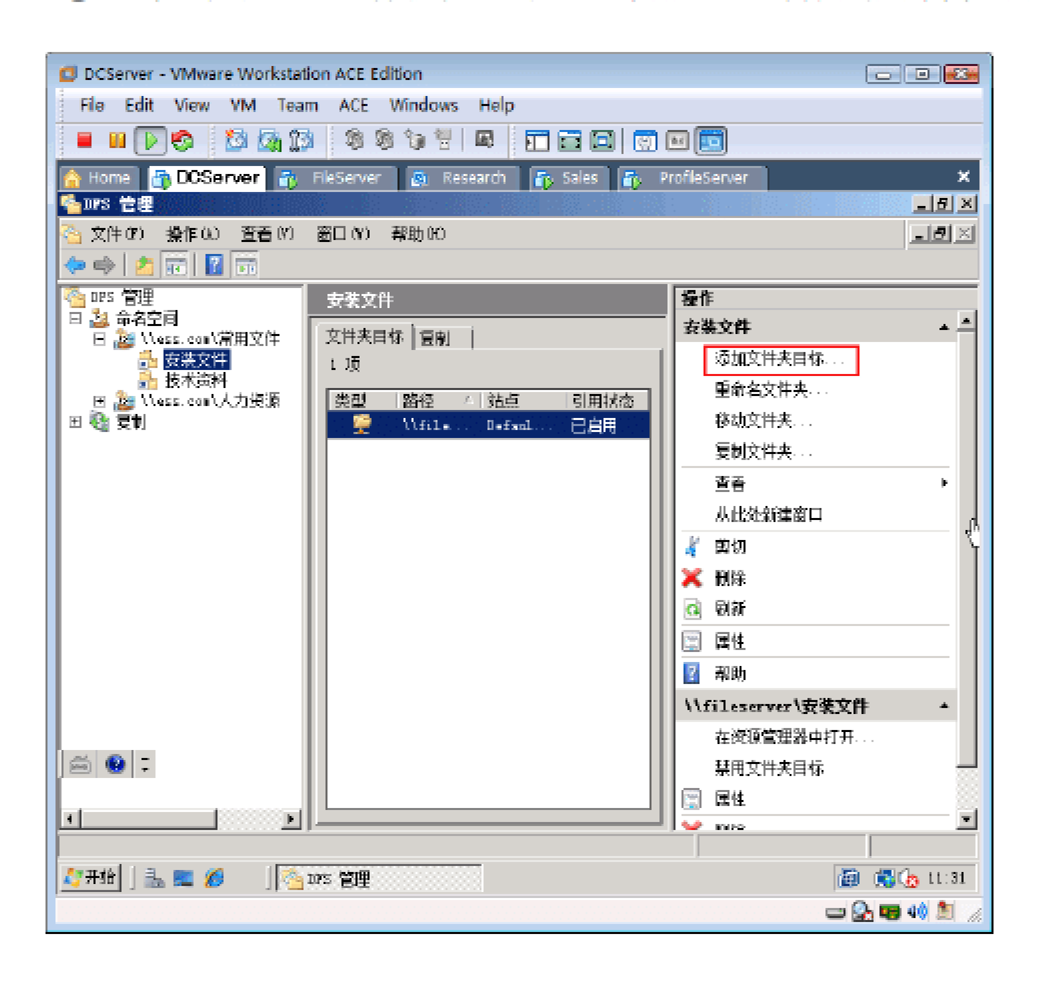


图 7-77　添加目标文件

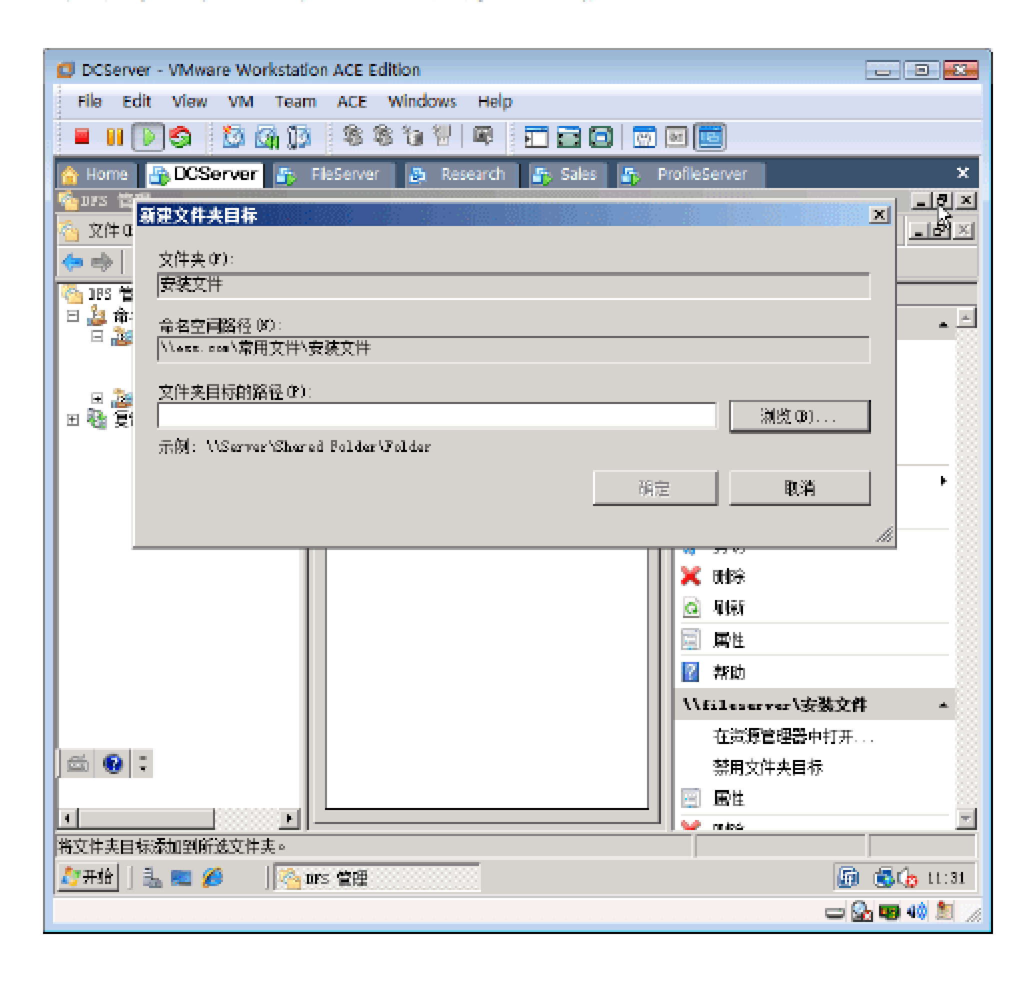


图 7-78　浏览目标文件夹

⑪　如图 7-79 所示，在“浏览共享文件夹”对话框的“服务器”文本框中输入 profileserver。单击“显示共享文件夹”按钮，发现没有共享的文件夹，然后单击“新建共享文件夹”按钮。

⑫　如图 7-80 所示，在“创建共享”对话框中输入共享名“安装文件”，单击“浏览”按钮。

⑬　如图 7-80 所示，在出现的“浏览文件夹”对话框中，选中 C$节点，单击“新建文件夹”按钮，输入文件夹的名称。单击“确定”按钮。

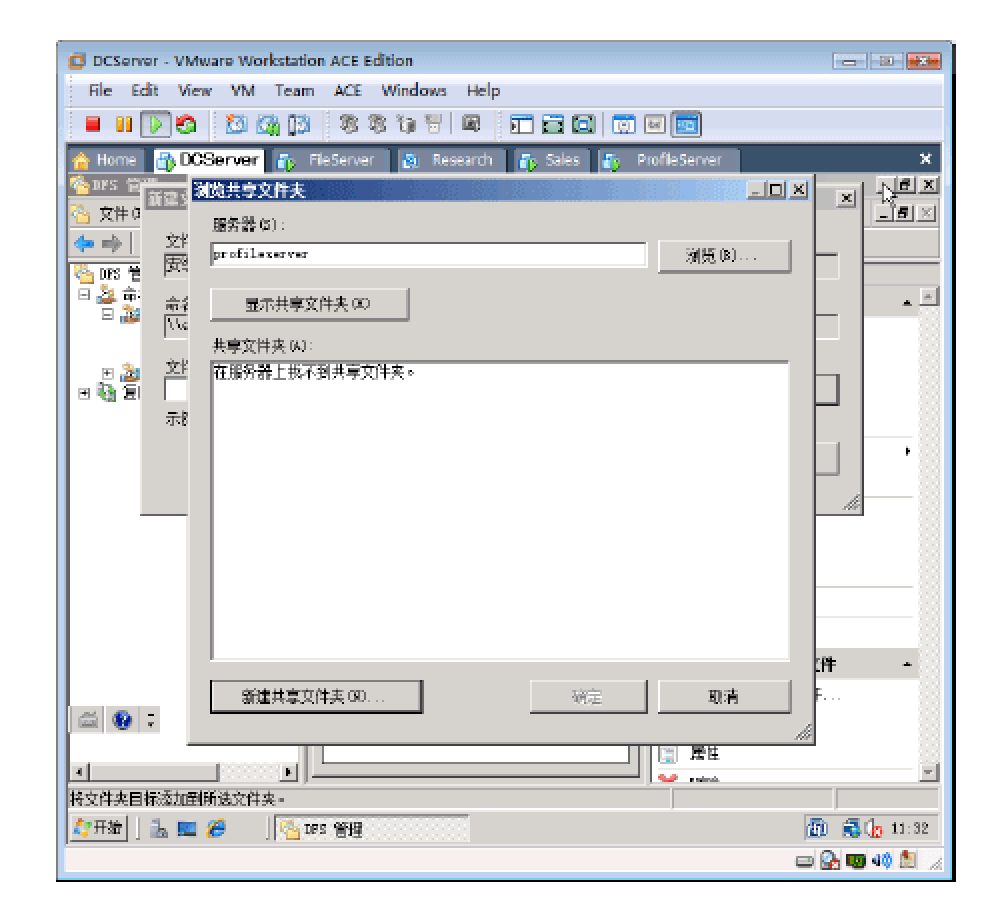


图 7-79　显示共享文件夹

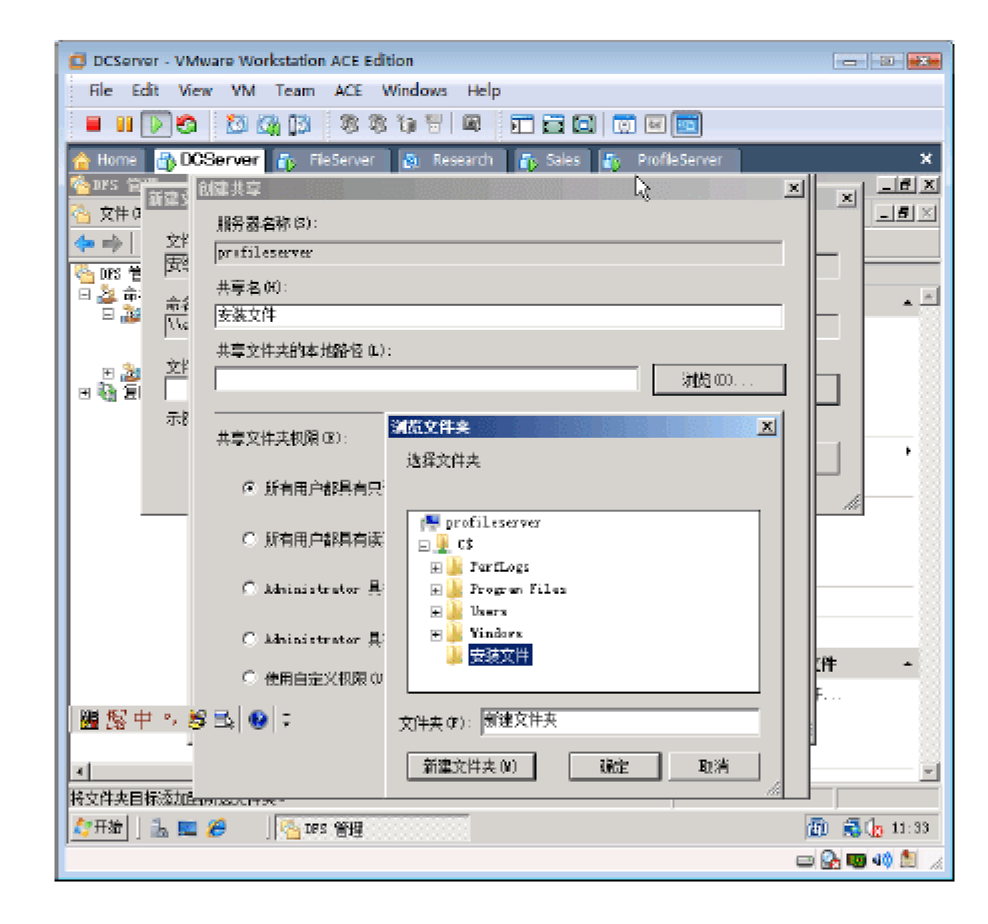


图 7-80　创建并共享文件夹

⑭ 如图 7-81 所示，在出现的“新建文件夹目标”对话框中单击“确定”按钮。

⑮ 如图 7-82 所示，在出现的“复制”对话框中单击“是”按钮。

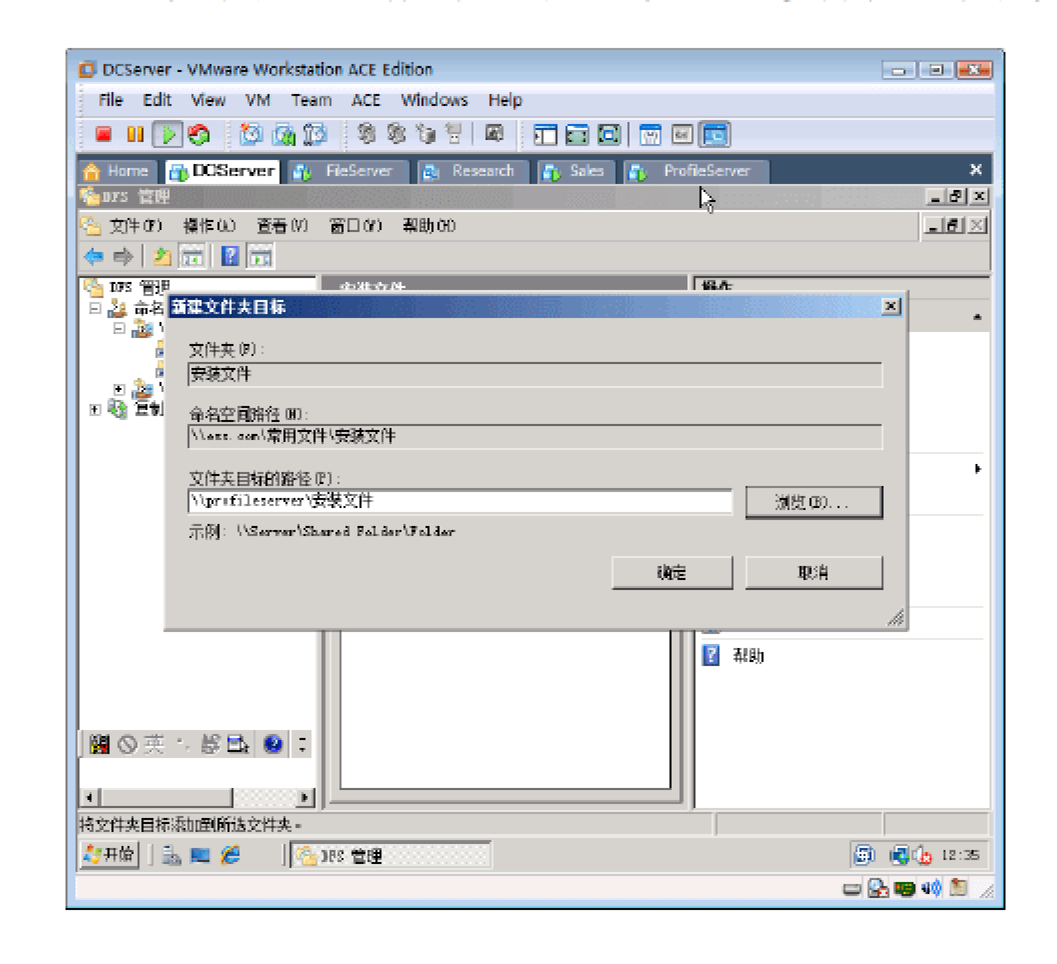


图 7-81 指定目标文件夹

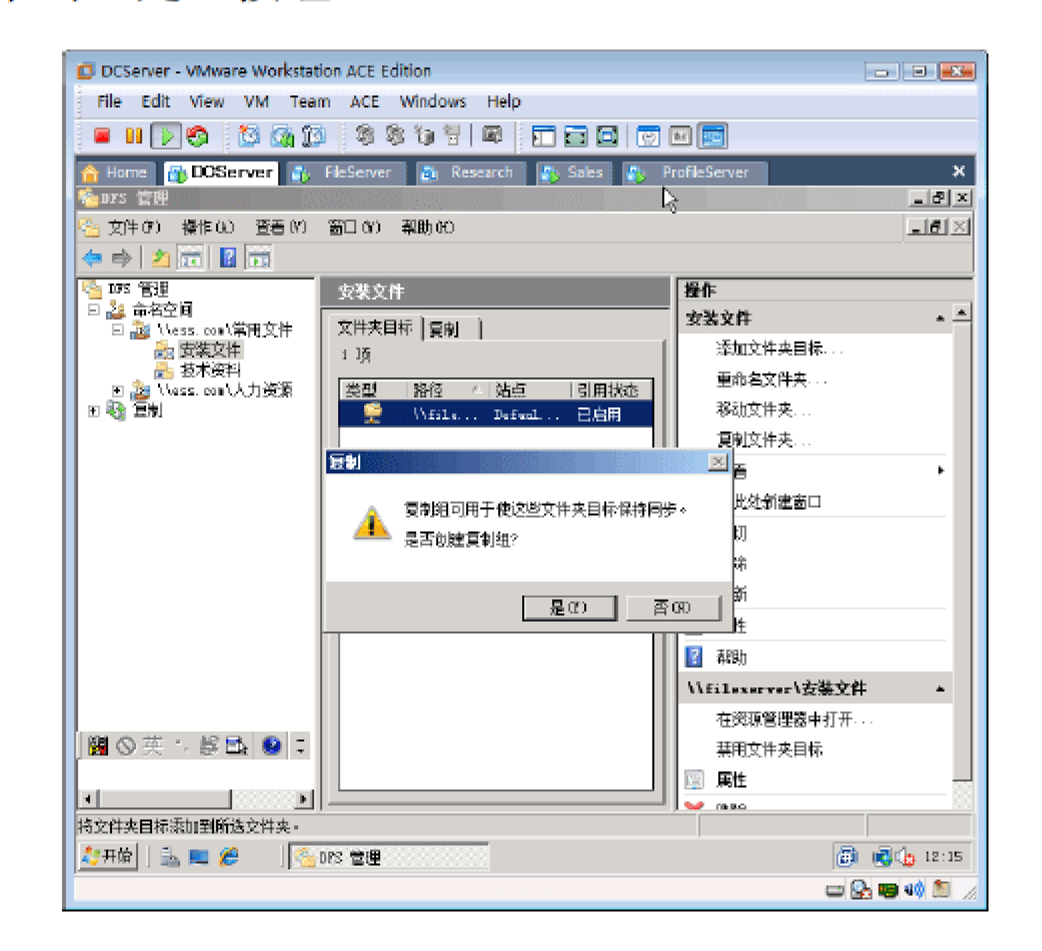


图 7-82 指定是否配置复制

⑯ 如图 7-83 所示，在“复制组和已复制文件夹名”界面中，单击“下一步”按钮。

⑰ 如图 7-84 所示，在“复制合格”界面中，单击“下一步”按钮。

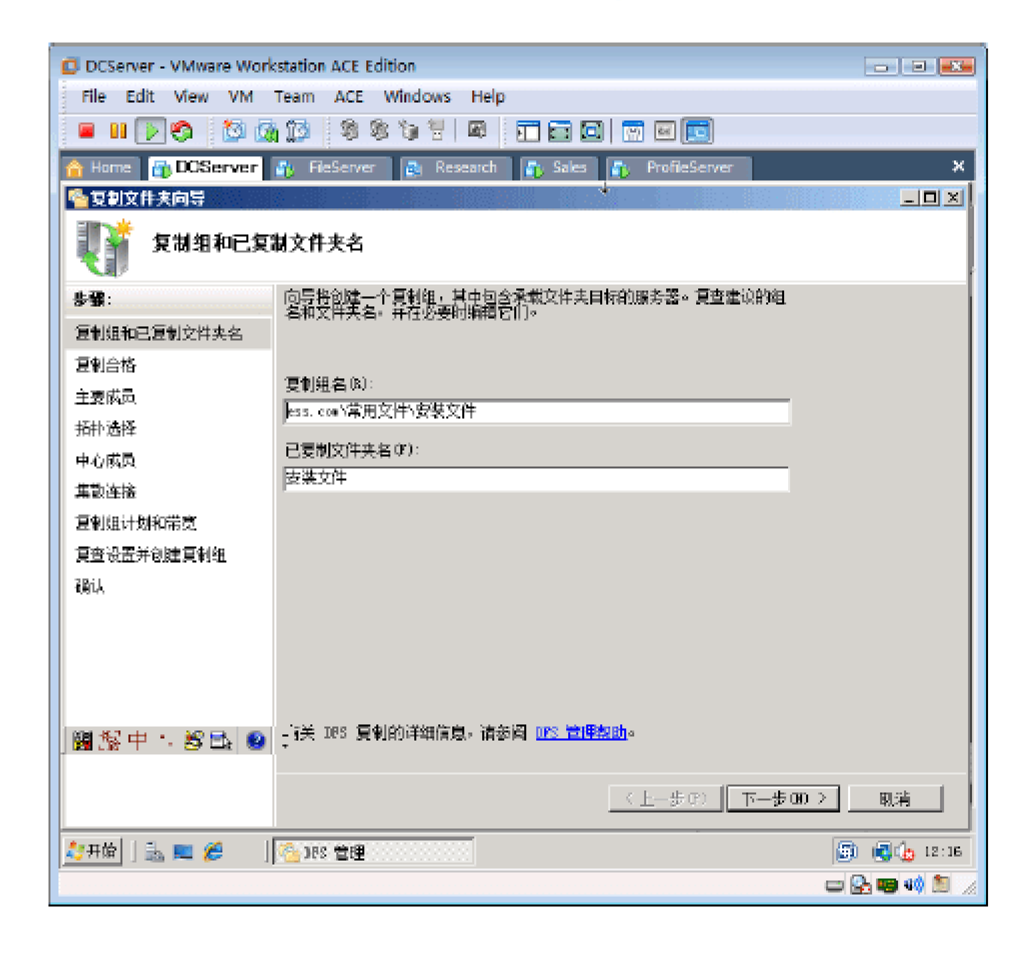


图 7-83 复制组

图 7-84 复制合格

⑱ 如图 7-85 所示，在出现的“主要成员”界面中，选中主要成员 FILESERVER。



注意：在这里指定的主要成员，只是在初次复制时以那个服务器的文件夹中的数据为主，配置好了之后，就不存在主和辅的区别，用户可以修改两个文件服务器上的文件，通过复制达到数据同步。

⑲ 如图 7-86 所示，在出现的“拓扑选择”界面中，选中“交错”单选按钮，单击“下一步”按钮。

⑳ 如图 7-87 所示，在“复制组计划和带宽”界面中，选中“使用指定带宽连续复制”单选按钮，单击“下一步”按钮。

㉑ 如图 7-88 所示，在“复查设置并创建复制组”对话框中，单击“创建”按钮。

㉒ 如图 7-89 所示，在“确认”对话框中，单击“关闭”按钮，完成添加目标文件夹。

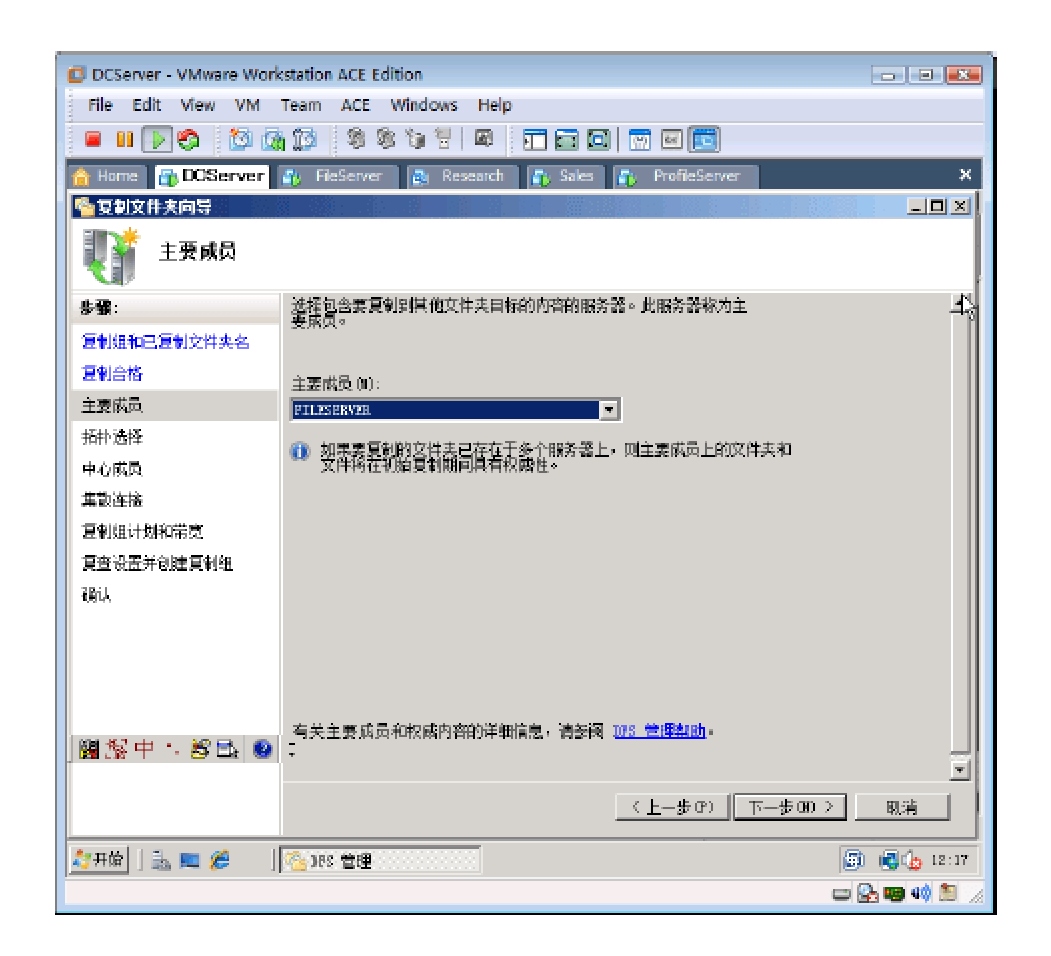


图 7-85　指定主要成员

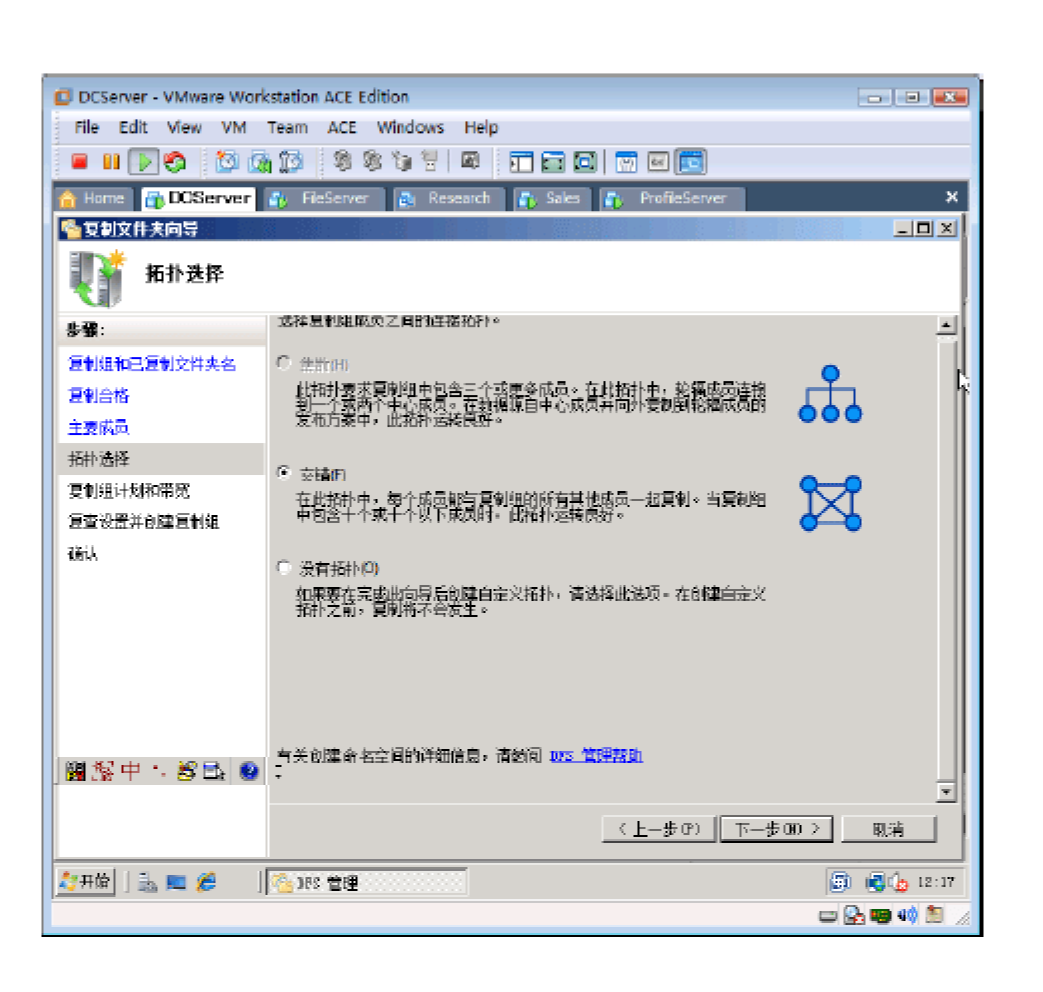


图 7-86　指定复制拓扑

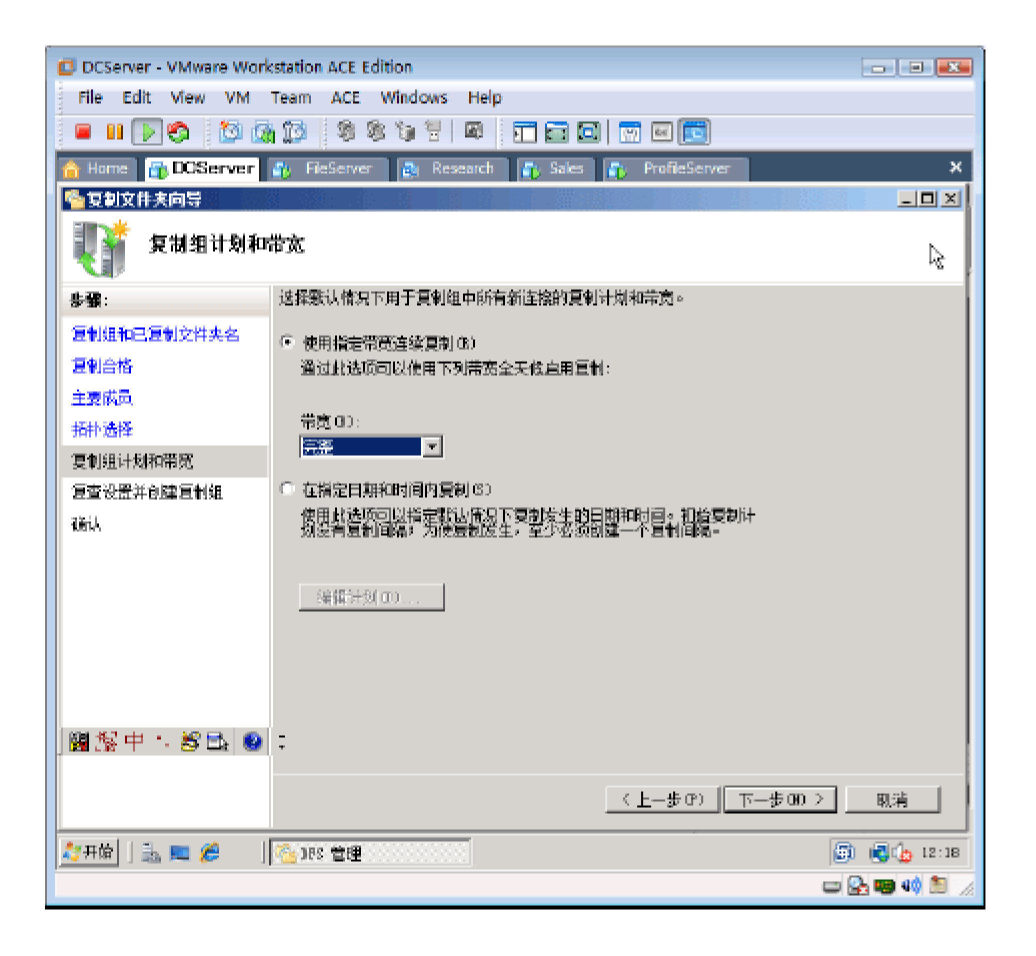


图 7-87　指定复制计划

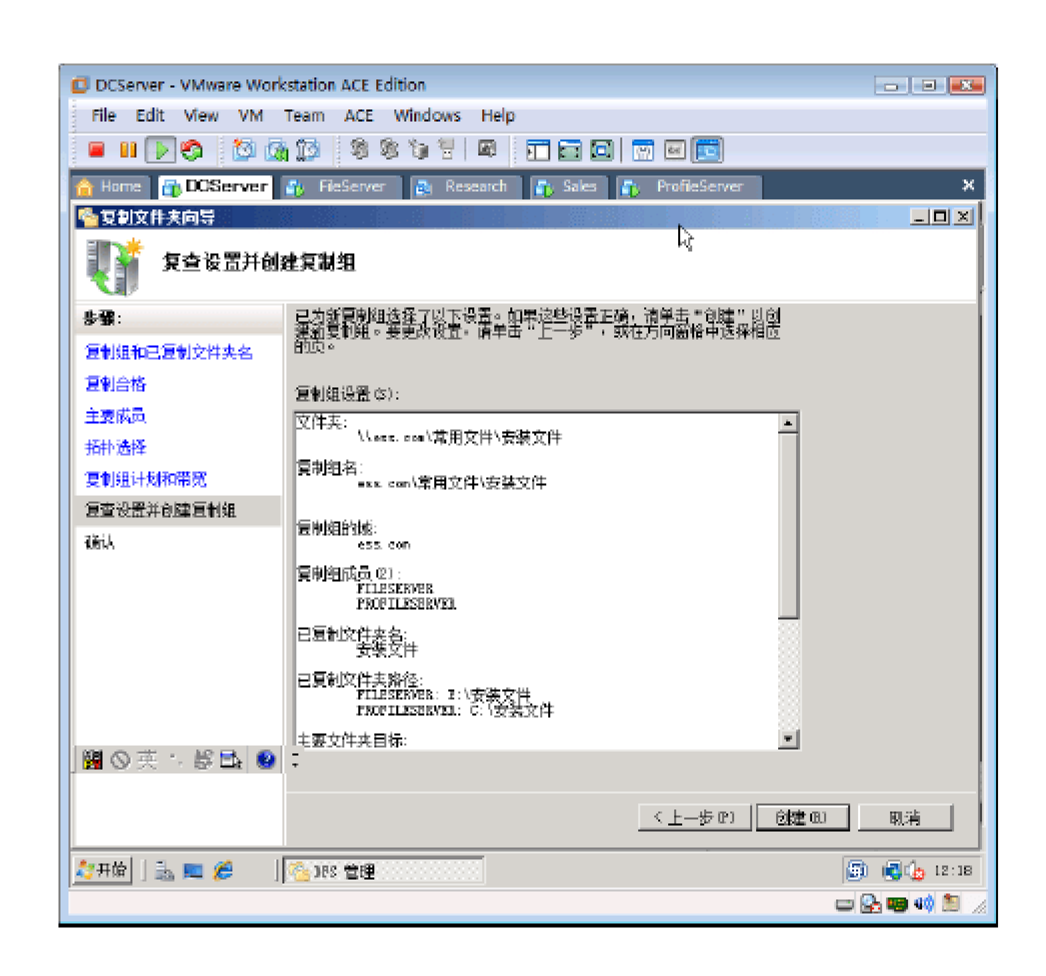


图 7-88　创建复制组

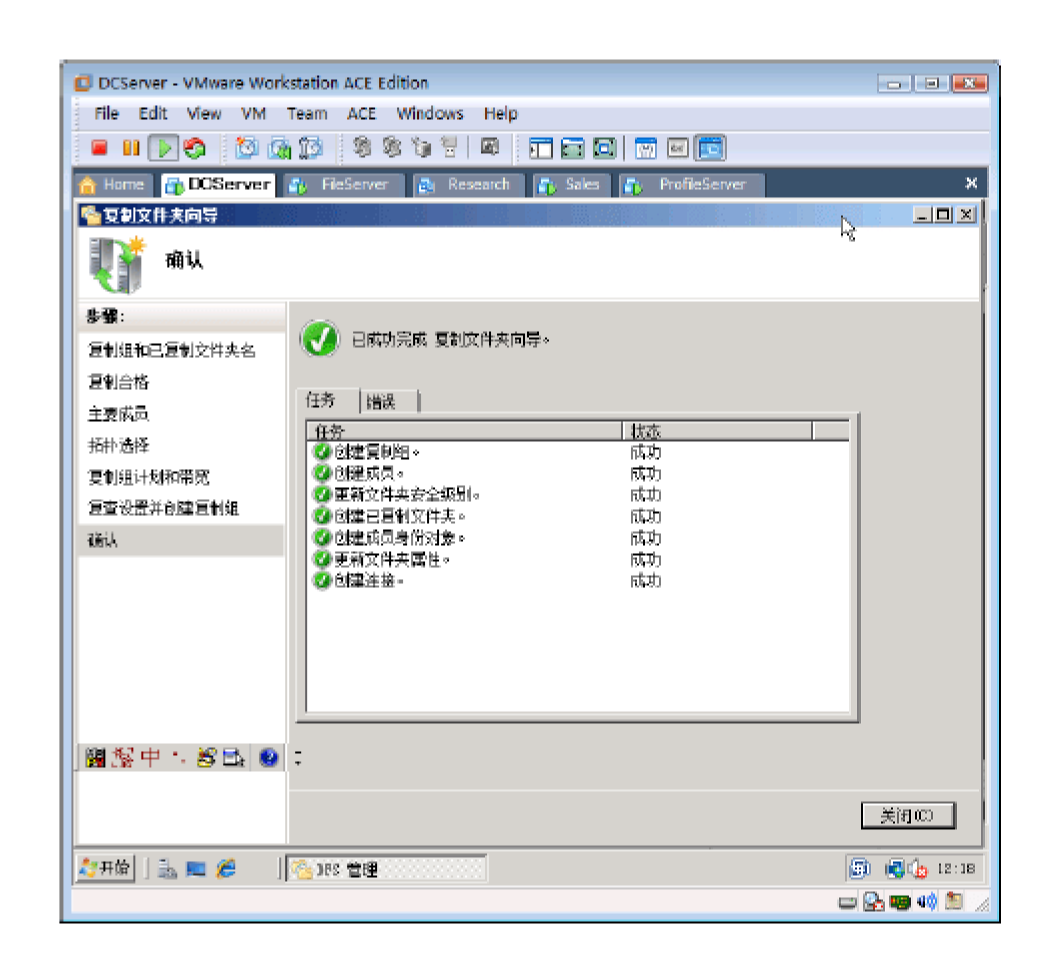


图 7-89　完成配置

7.3.5 任务 5：验证 DFS 的复制和容错

验证“安装文件”的复制和容错

① 以域管理员用户账户登录到 FileServer。

② 在 E 盘“安装文件”中创建一个记事本文件 FileServer.txt。

③ 选择“开始”→“运行”命令，在“运行”对话框中输入“\\profileserver\安装文件”。

④ 可以发现，在 ProfileServer 服务器的安装文件上也会立即出现，如图 7-90 所示。

⑤ 如图 7-91 所示，选择 VM→Removable Devices→Ethernet→Disconnect 命令，断开 FileServer 服务器的网卡连接，这样用户就不能访问其共享的“安装文件”了。

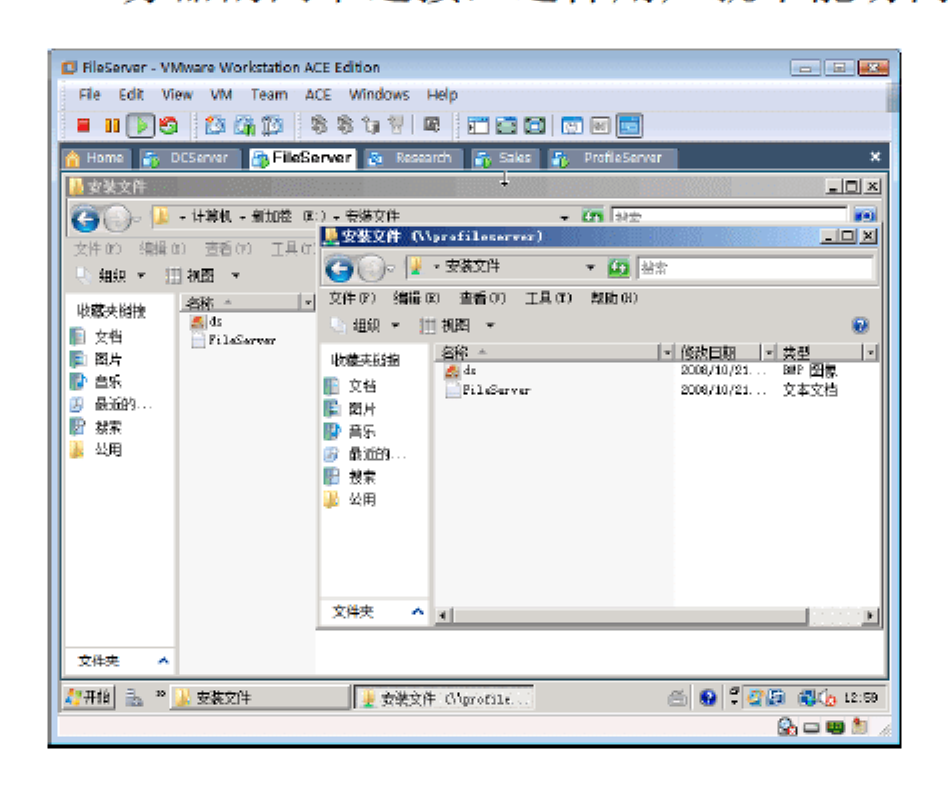


图 7-90 两个服务器上的安装文件同步

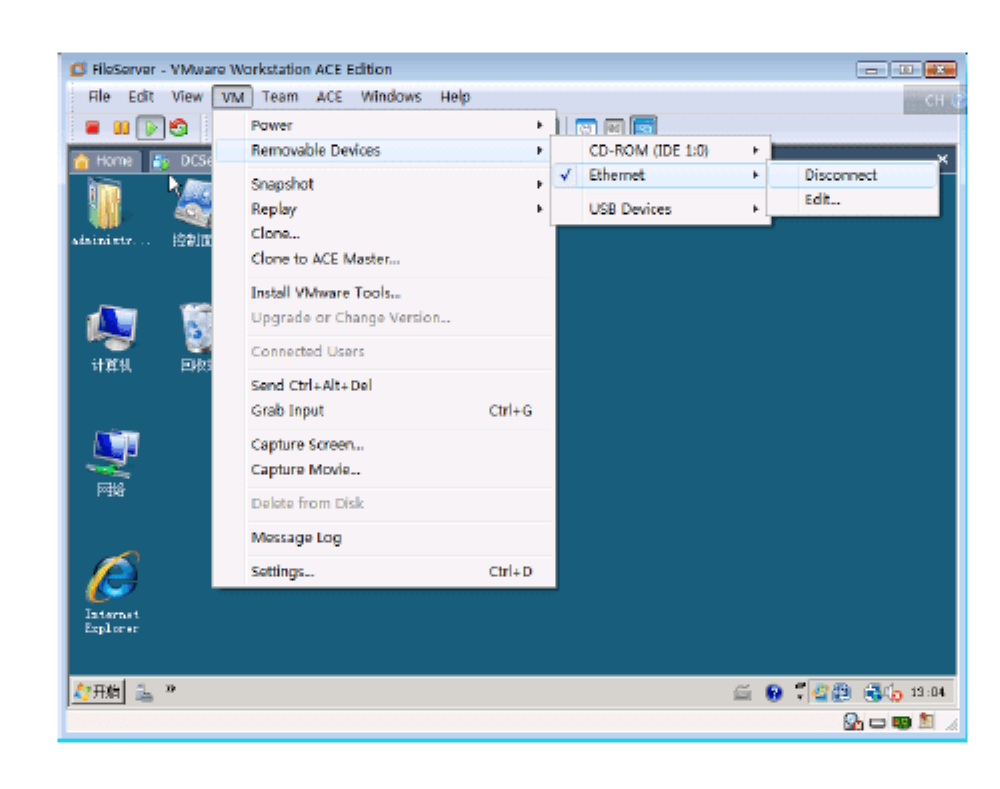


图 7-91 断开网卡连接

⑥ 在 Sales 计算机访问“\\Ess.com\常用文件”文件夹中的“安装文件”，发现等稍长的时间用户还是能够打开“安装文件”子文件夹。

7.3.6 任务 6：管理 DFS 复制

DFS 中多个目标文件夹默认是相互复制的，可以禁用某个复制，形成单向复制。

① 如图 7-92 所示，右击接收成员 FileServer，从弹出的快捷菜单中选择“禁用”命令，这样只能实现 FileServer 到 ProfileServer 的复制。

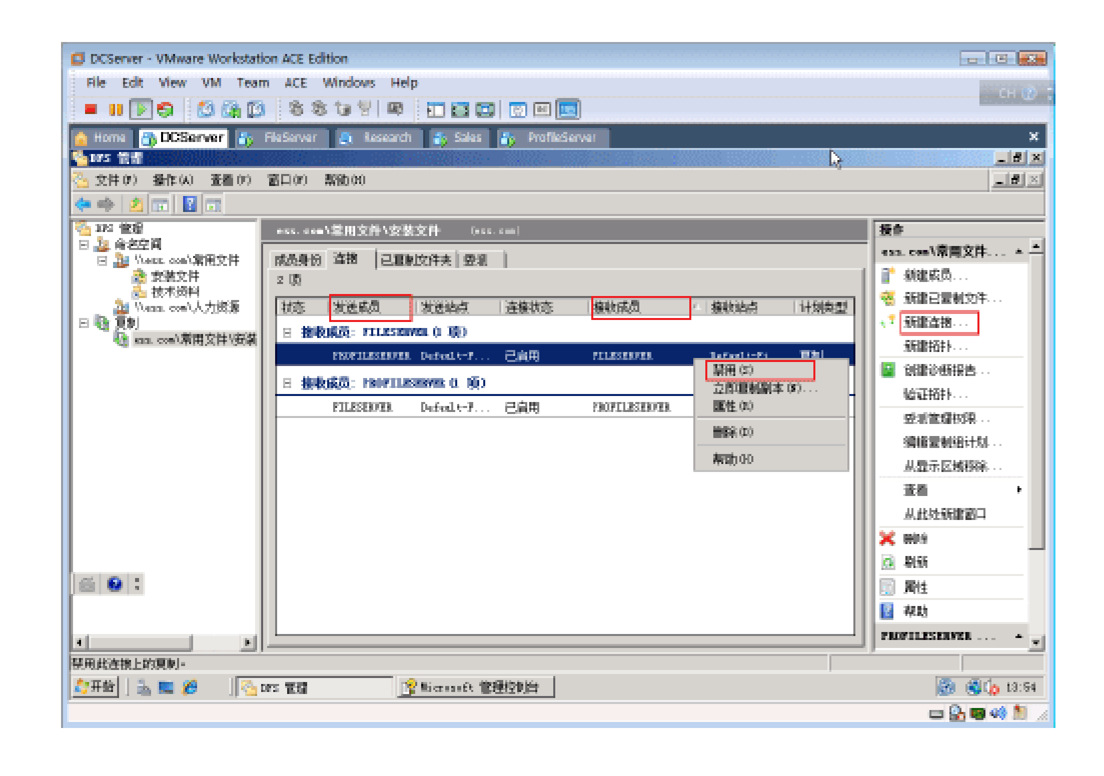


图 7-92 管理 DFS 复制

② 如图 7-92 所示，也可以选择“立即复制副本”命令。如果选择“删除”命令，可以删除连接。

③ 如图 7-93 所示，单击“新建连接”按钮，在出现的对话框中，可以指定发送成员，接收成员，如果不选中“在相反方向创建另一个连接”复选框，只能创建单向连接。

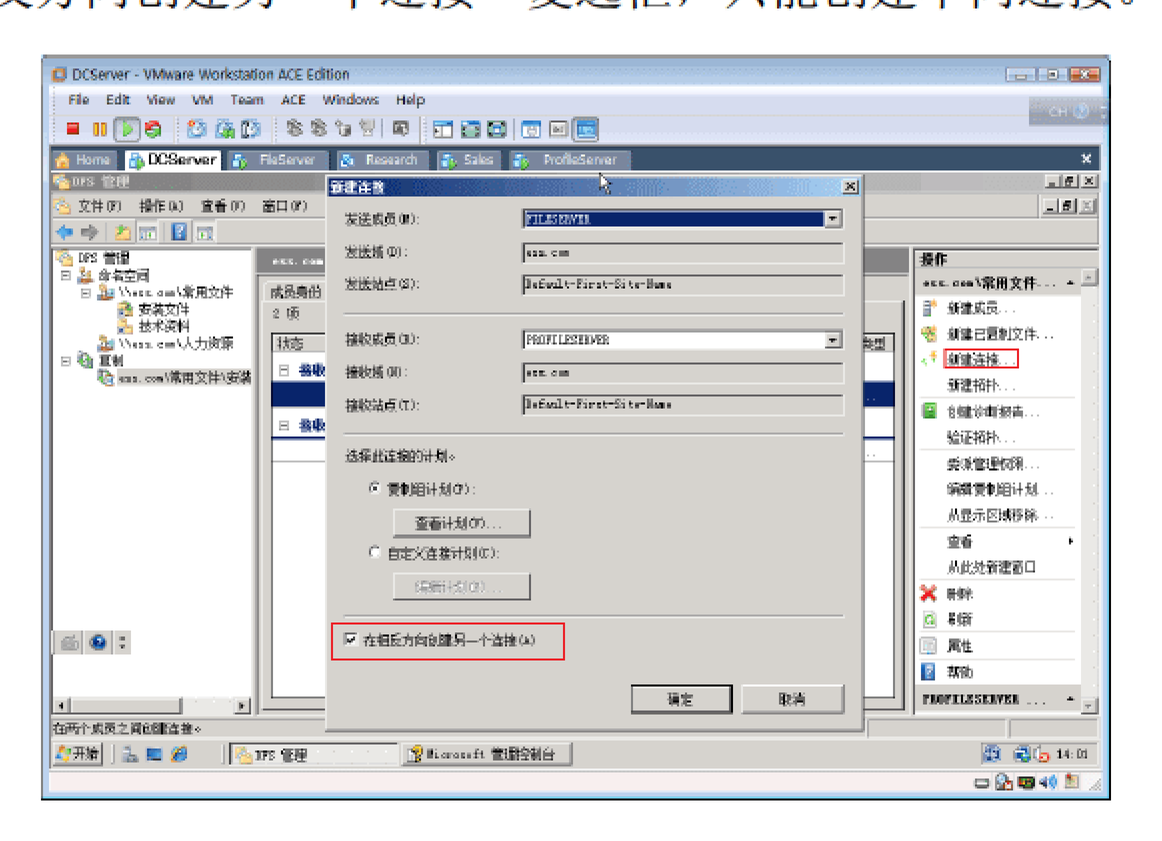


图 7-93 创建 DFS 连接

7.3.7 任务 7：支持分支办公室

如图 7-94 所示，某公司创建了一个 Ess.com 域，分公司在石家庄，网络中心在北京。分公司和网络中心通过广域网连接，网络中心的子网为 10.7.10.0，255.255.255.0，分公司的子网为 192.168.1.0，255.255.255.0。

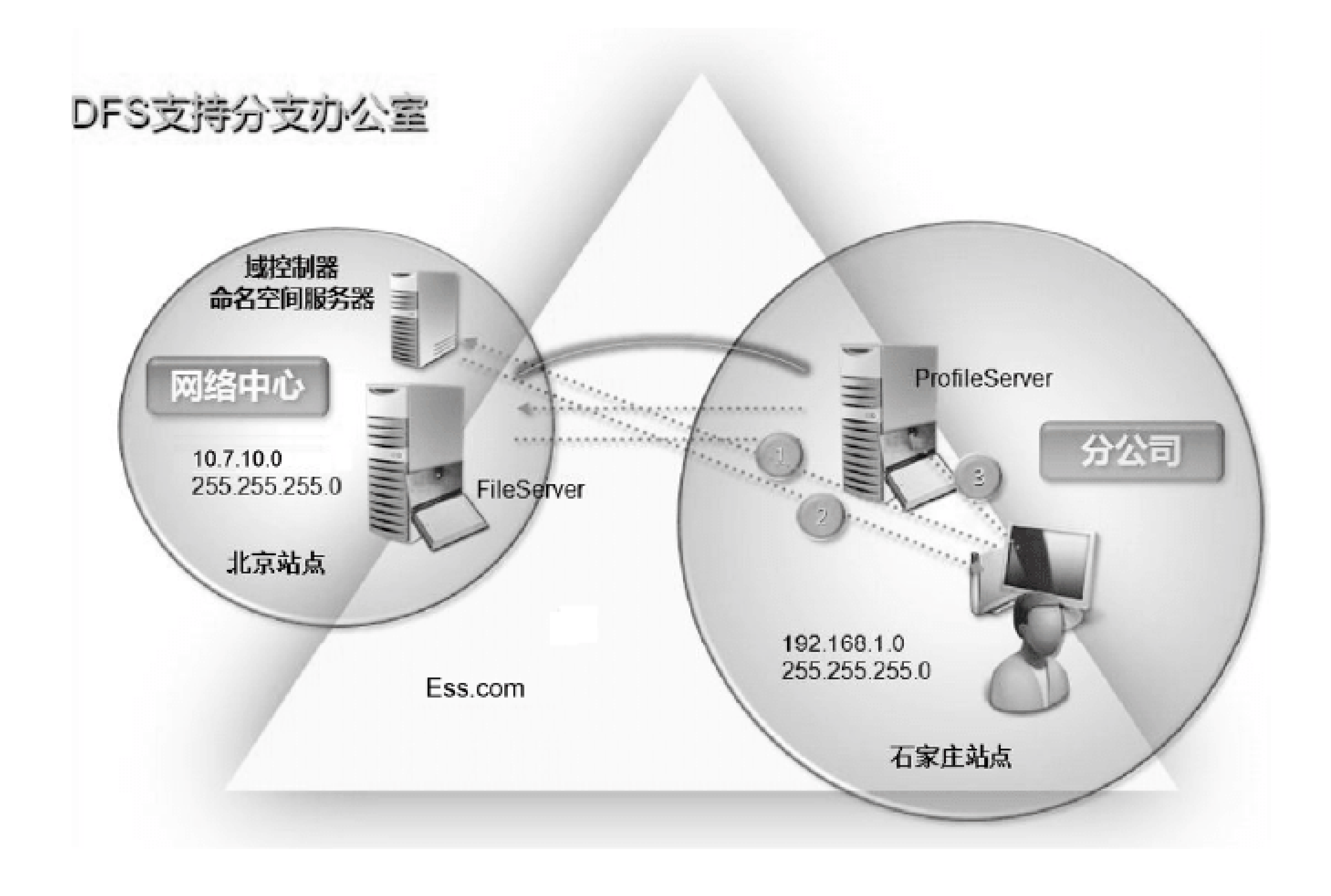


图 7-94 公司物理网络拓扑

公司的“安装文件”文件夹存放在 FileServer 服务器上，分公司用户访问 FileServer 要跨越广域网，速度较慢。为了方便分公司的员工访问公司“安装文件”，在分公司的文件服务器 ProfileServer 上创建“安装文件”文件夹并共享，然后利用 DFS 将“安装文件”在这两个服务器上同步。

当石家庄的用户访问输入“\\Ess.com\常用文件”访问该域中的命名空间时，用户最好被定位到位于石家庄站点的 ProfileServer 服务器上。当北京的用户访问输入“\\Ess.com\常用文件”访问该域的命名空

间时，最好被定位到位于北京站点的 FileServer 服务器上。要实现将用户自动定位到同一站点的服务器上，需要配置活动目录站点和子网对象。这样命名空间服务器将会根据用户计算机的 IP 地址，将用户定位到同一站点的文件服务器上。

首先，按照图 7-95 配置计算机的 IP 地址。需要在 DCServer 计算机的网络连接中添加两个 IP 地址，来模拟两个网卡，然后将其配置成路由器，允许在网络中心和分公司之间转发数据包。

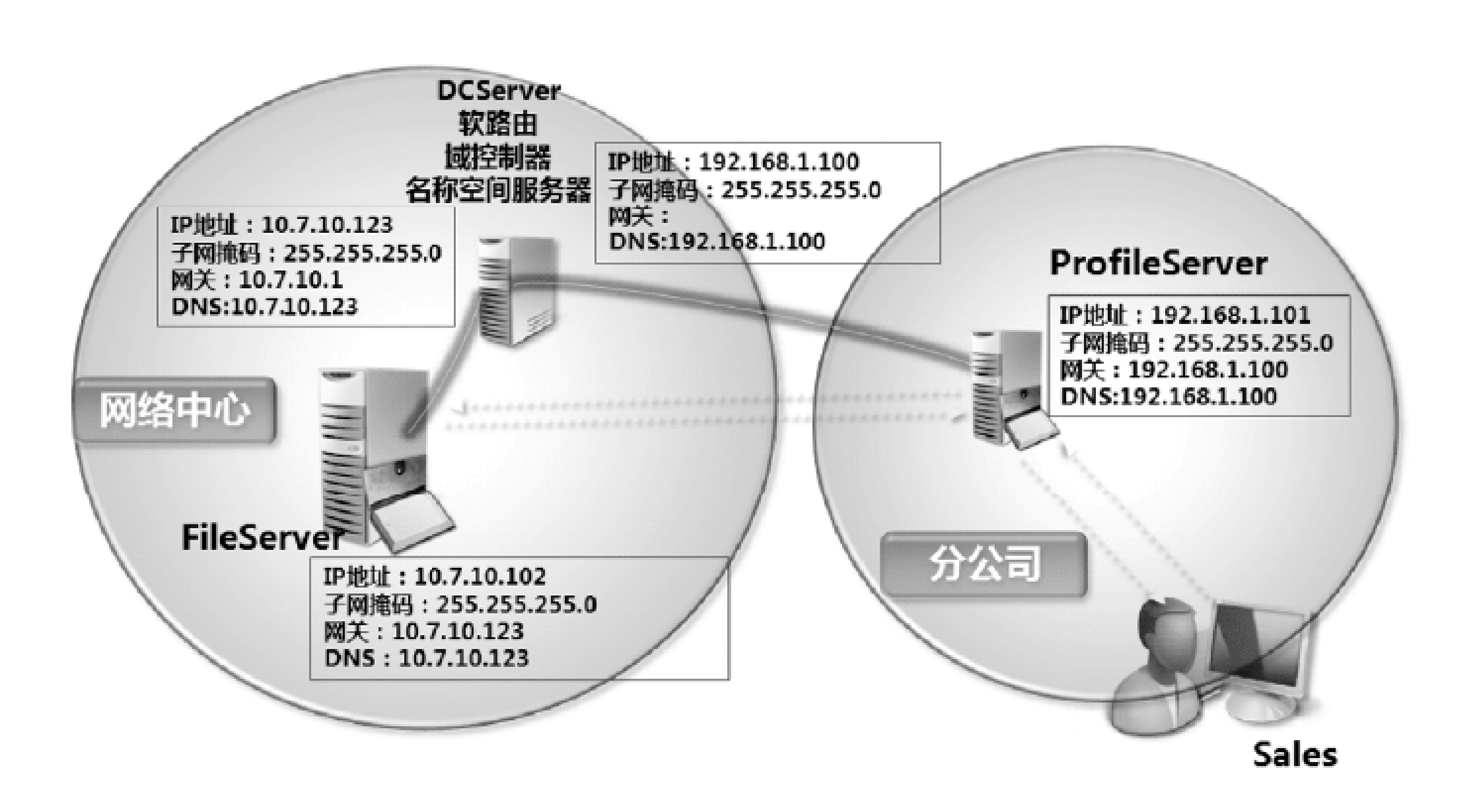


图 7-95　试验环境

然后在 DCServer 上安装路由和远程访问服务，并启用路由功能，然后创建活动目录站点和子网对象。

① 以域管理员的身份登录到域控制器 DCServer 上。

② 打开服务器管理器，单击“服务器角色”，单击“添加角色”。在出现的对话框中，单击“下一步”按钮。

③ 如图 7-96 所示，在“选择服务器角色”界面中，选中“网络策略和访问服务”复选框，单击“下一步”按钮。

④ 如图 7-97 所示，在出现的“选择角色服务”界面中，选中“路由”和“远程访问服务”复选框，单击“下一步”按钮，在“确认选择”界面中，单击“安装”按钮，完成安装。

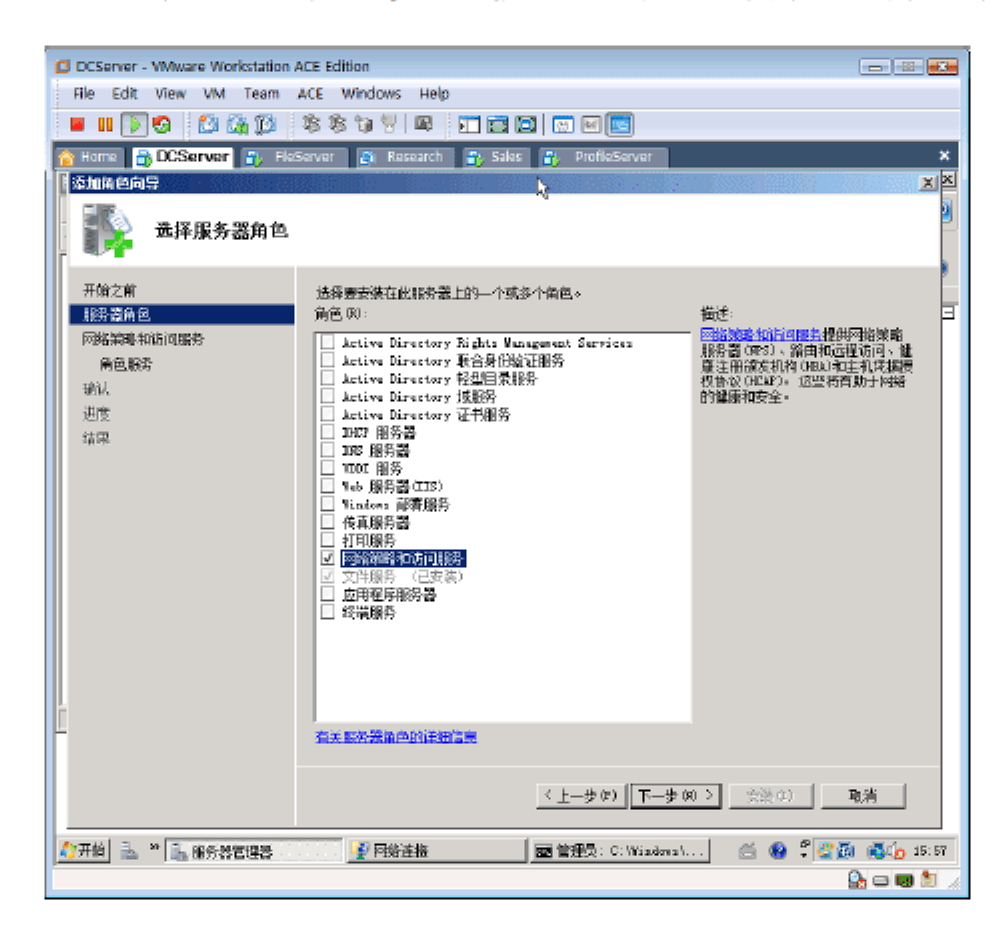


图 7-96　安装角色

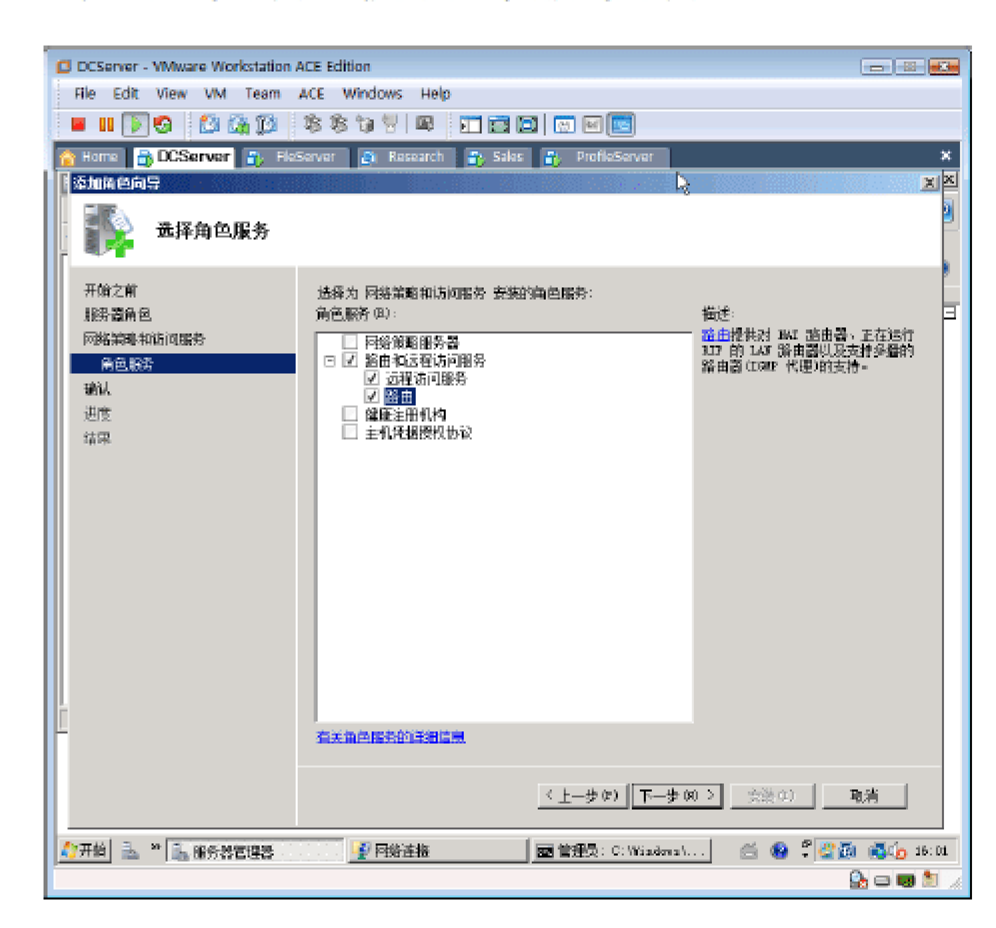


图 7-97　选择角色服务

⑤ 选择“开始”→“程序”→“管理工具”→“路由和远程访问”命令。

⑥ 如图 7-98 所示，右击 DCSERVER 服务器，在弹出的快捷菜单中选择“配置并启用路由和远程访问”命令。

⑦ 如图 7-99 所示，在出现的“配置”界面中，选中“自定义配置”单选按钮，单击“下一步”按钮。

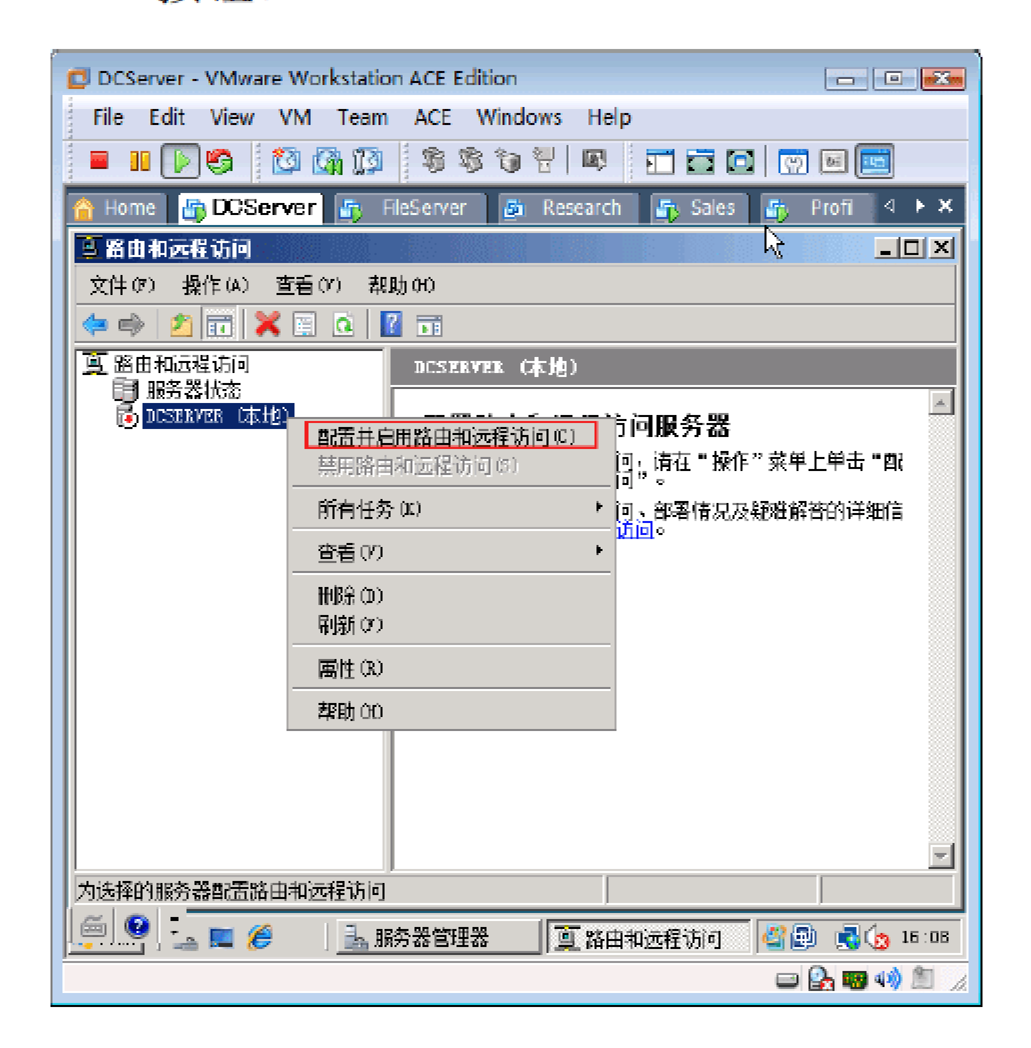


图 7-98　配置路由和远程访问

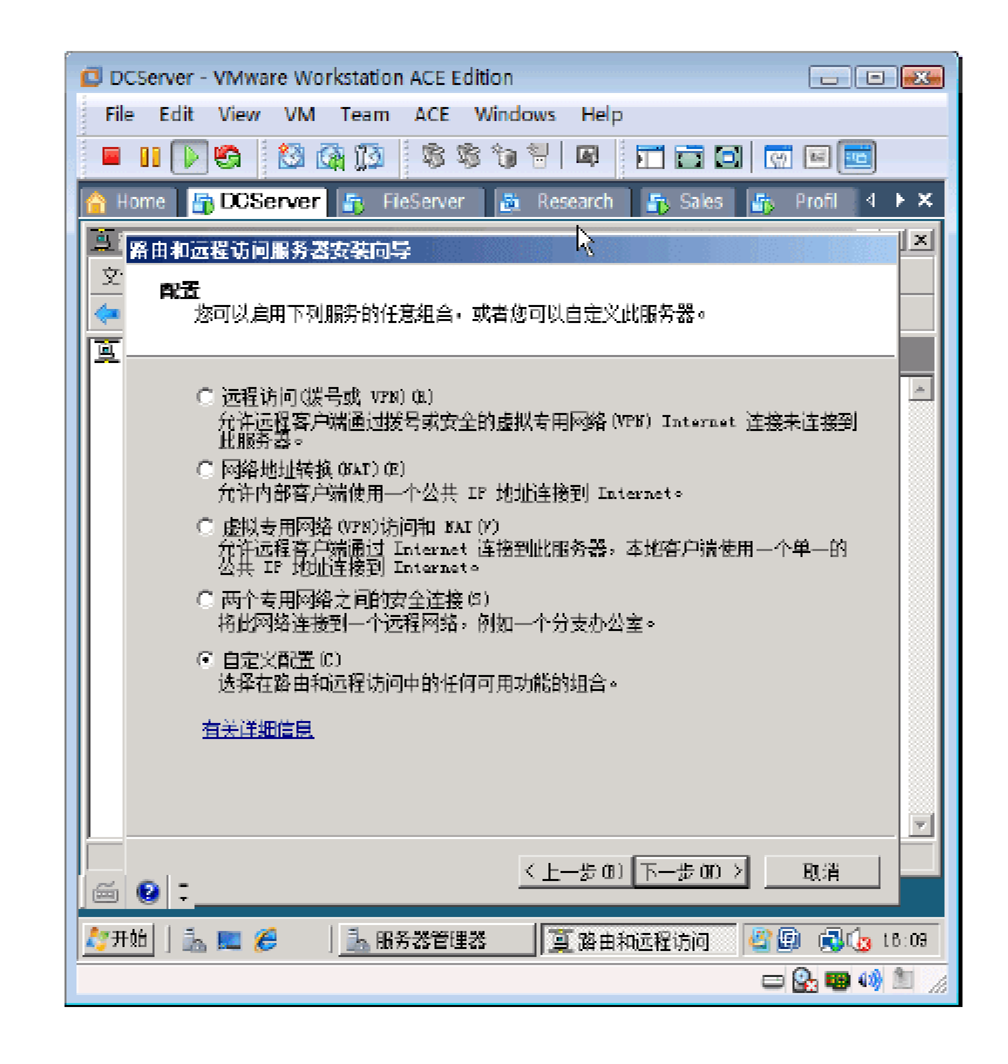


图 7-99　自定义配置

⑧ 如图 7-100 所示，在“自定义配置”界面中，选中“LAN 路由”复选框，单击“下一步”按钮，完成配置。现在已经将 DCSERVER 配置成路由器了，通常将 Windows 配置成的路由器称为软路由。

⑨ 选择“开始”→“程序”→“管理工具”→“Active Directory 站点和服务”命令。

⑩ 如图 7-101 所示，右击 Default-First-Site-Name，在弹出的快捷菜单中选择“重命名”命令，在出现的对话框中输入“北京”。

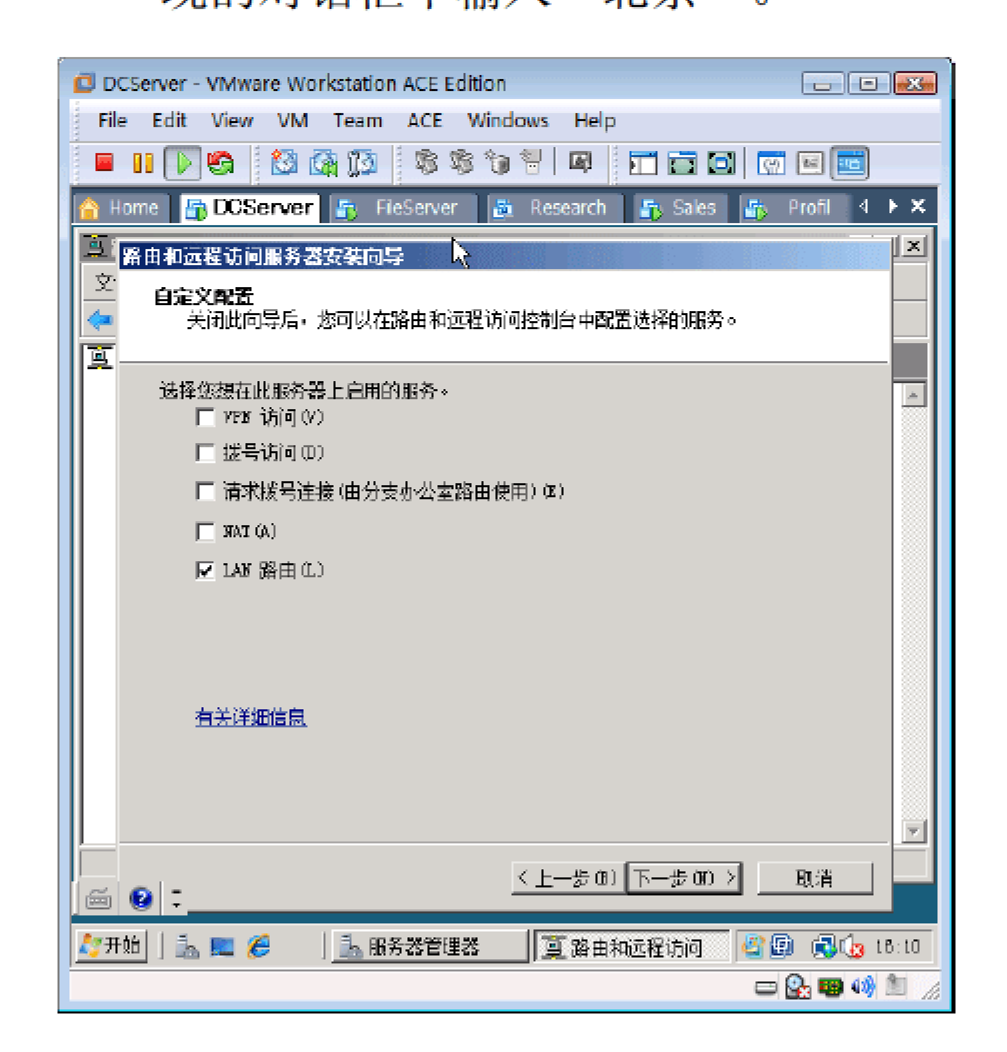


图 7-100　路由

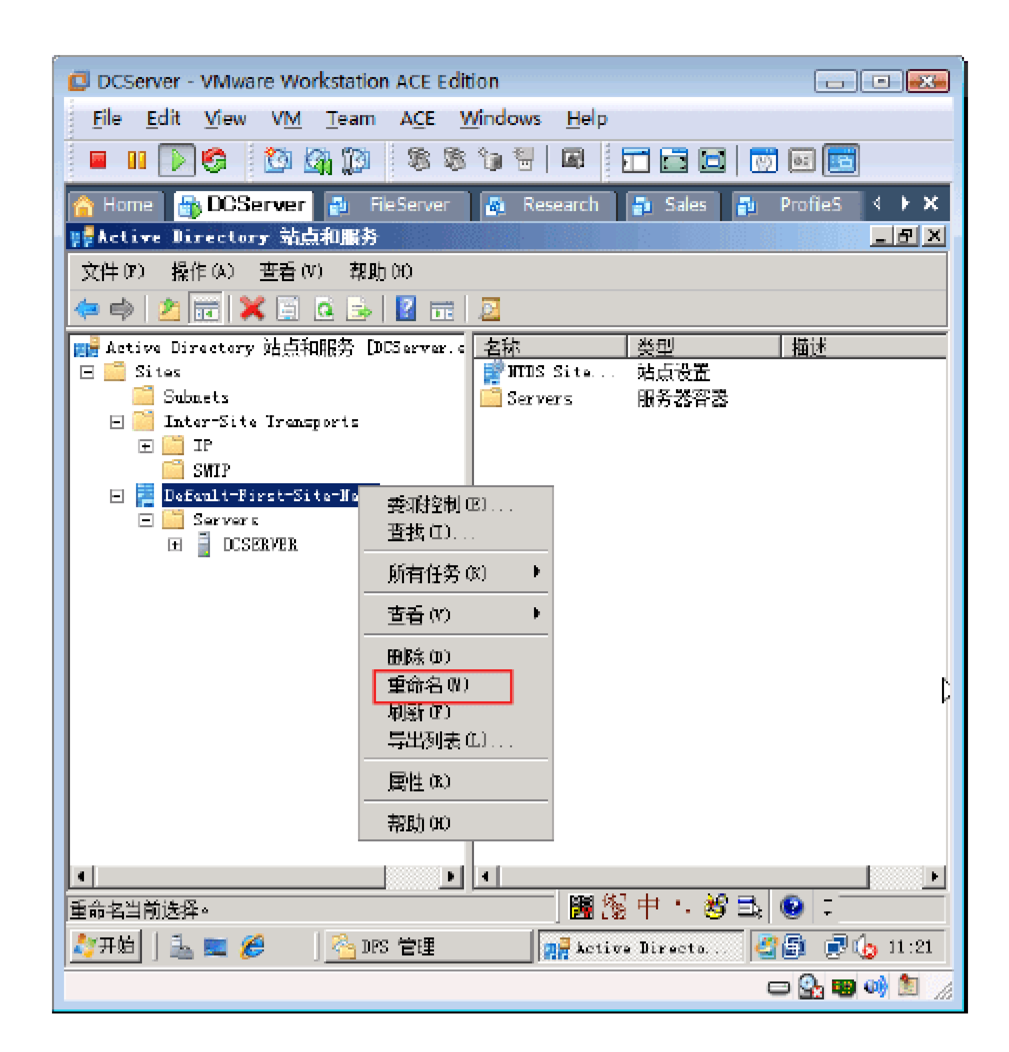


图 7-101　重命名默认活动目录站点

⑪ 如图 7-102 所示，重命名完成。

⑫ 如图 7-103 所示，右击 Sites，在弹出的快捷菜单中选择“新站点”命令，在出现的对话框中输入“石家庄”，选中下面的连接 DEFAULTIPSITELINK，如图 7-104 所示。单击“确定”按钮。

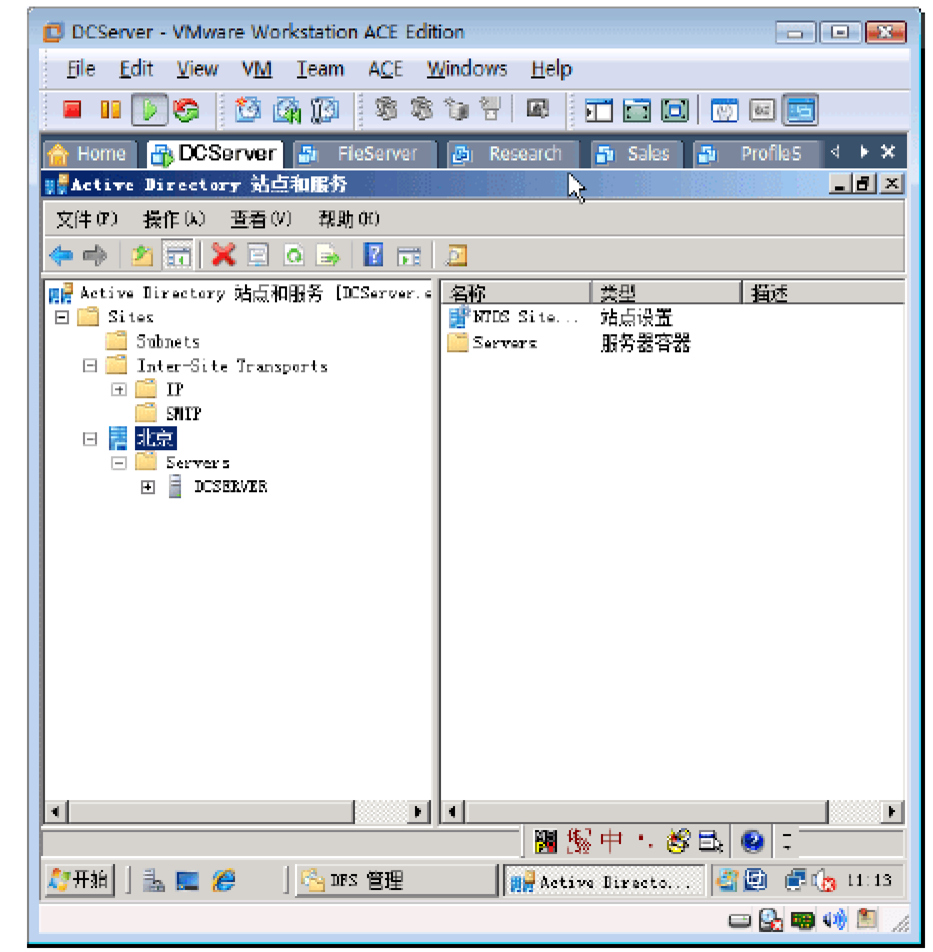


图 7-102　站点被重命名

图 7-103　新建活动目录站点

⑬ 出现提示对话框，单击“确定”按钮。

⑭ 如图 7-105 所示，右击 Subnets，在弹出的快捷菜单中选择“新建子网”命令，在出现的对话框中输入 10.7.10.0/24，选中“北京”站点，单击“确定”按钮，如图 7-106 所示。

⑮ 如图 7-107 所示，创建子网对象 192.168.1.0/24，选中“石家庄”站点，单击“确定”按钮。

⑯ 如图 7-108 所示，再次打开 DFS 会发现，“安装文件”的文件夹目标，FileServer 服务器在北京站点，ProfileServer 服务器在石家庄站点。这说明活动目录根据服务器的 IP 地址对照活动目录站点子网对象将其划分到不同的站点中。

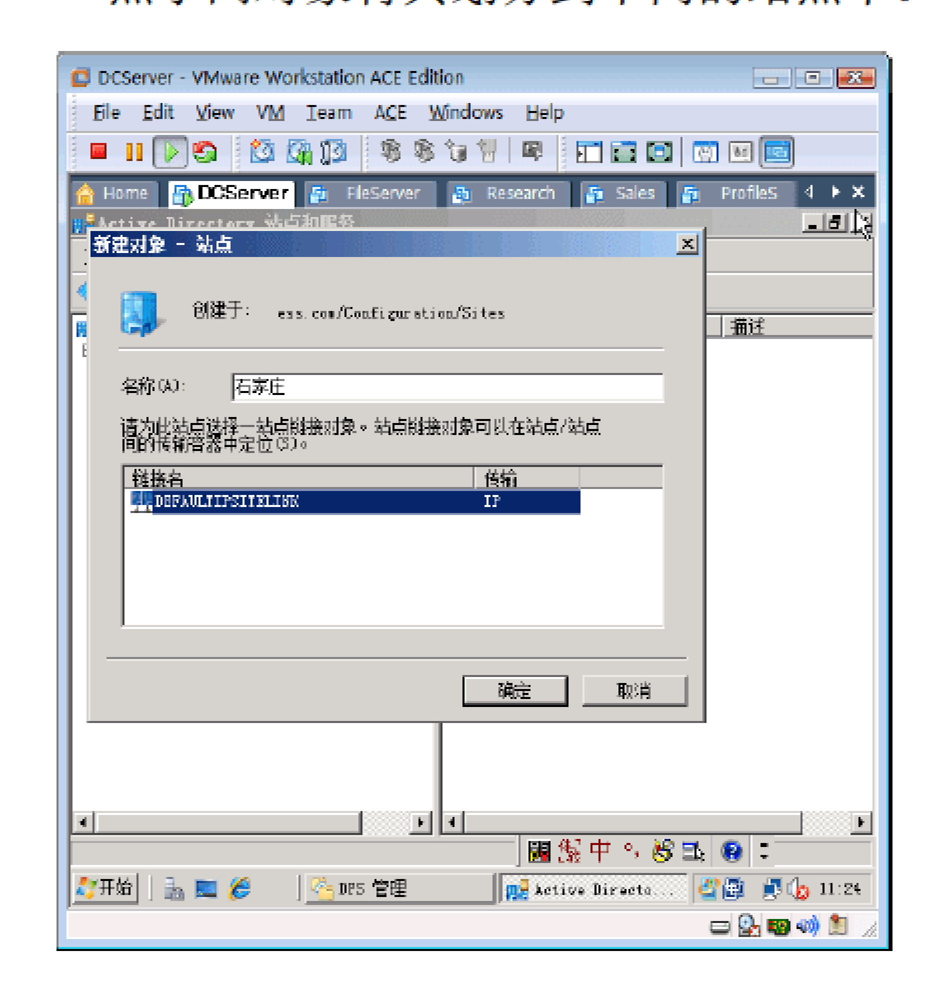


图 7-104　选择站点间连接

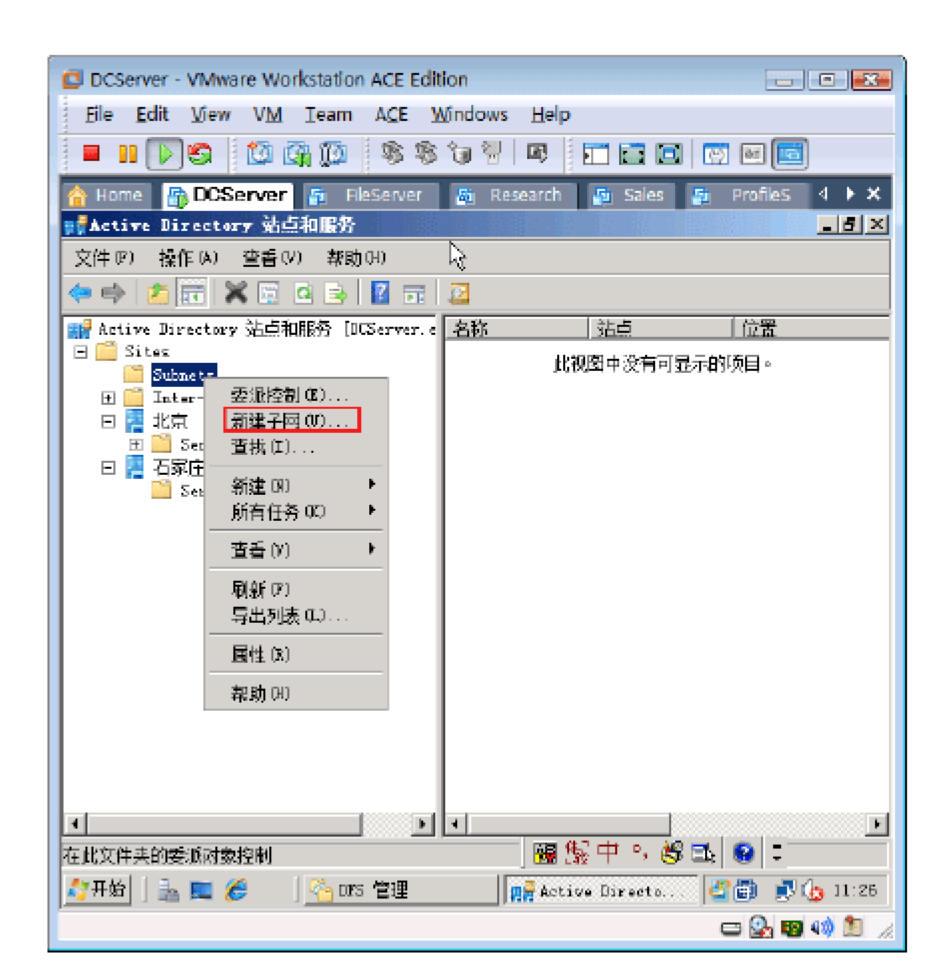


图 7-105　创建子网对象

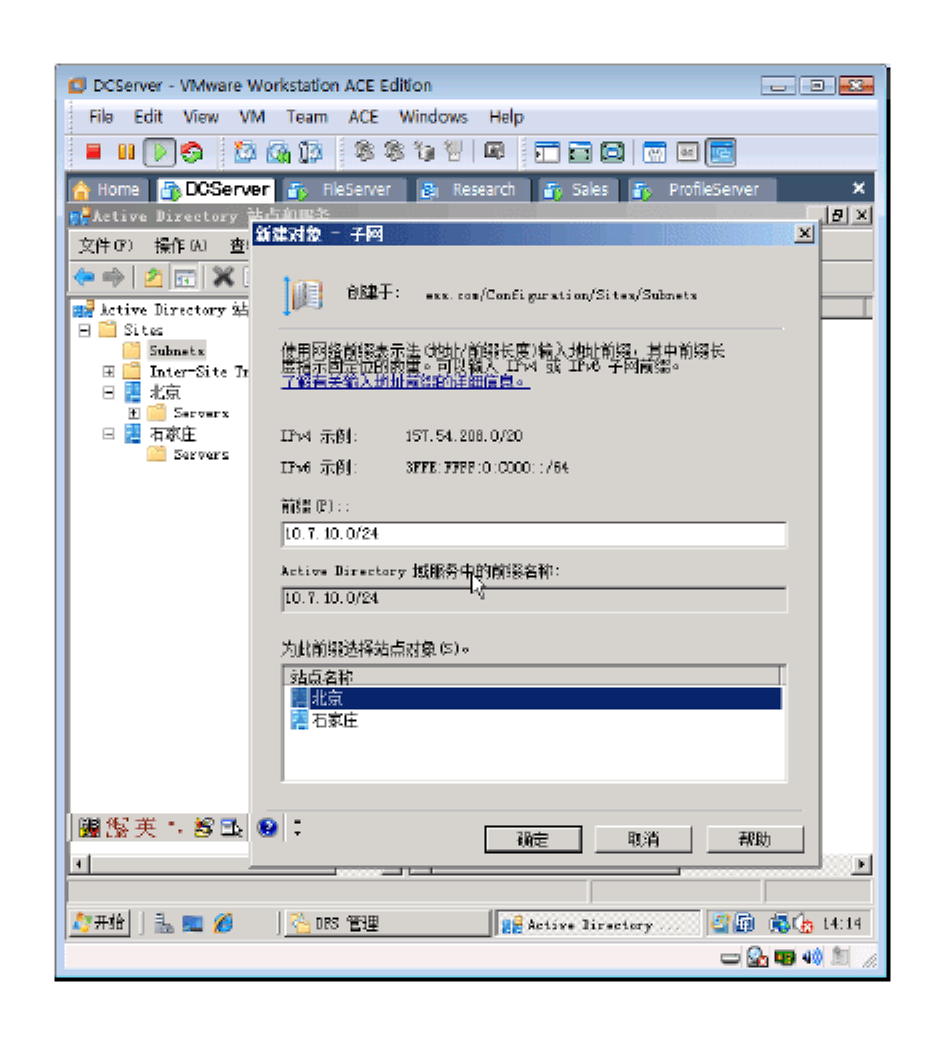


图 7-106　指定子网所处的站点

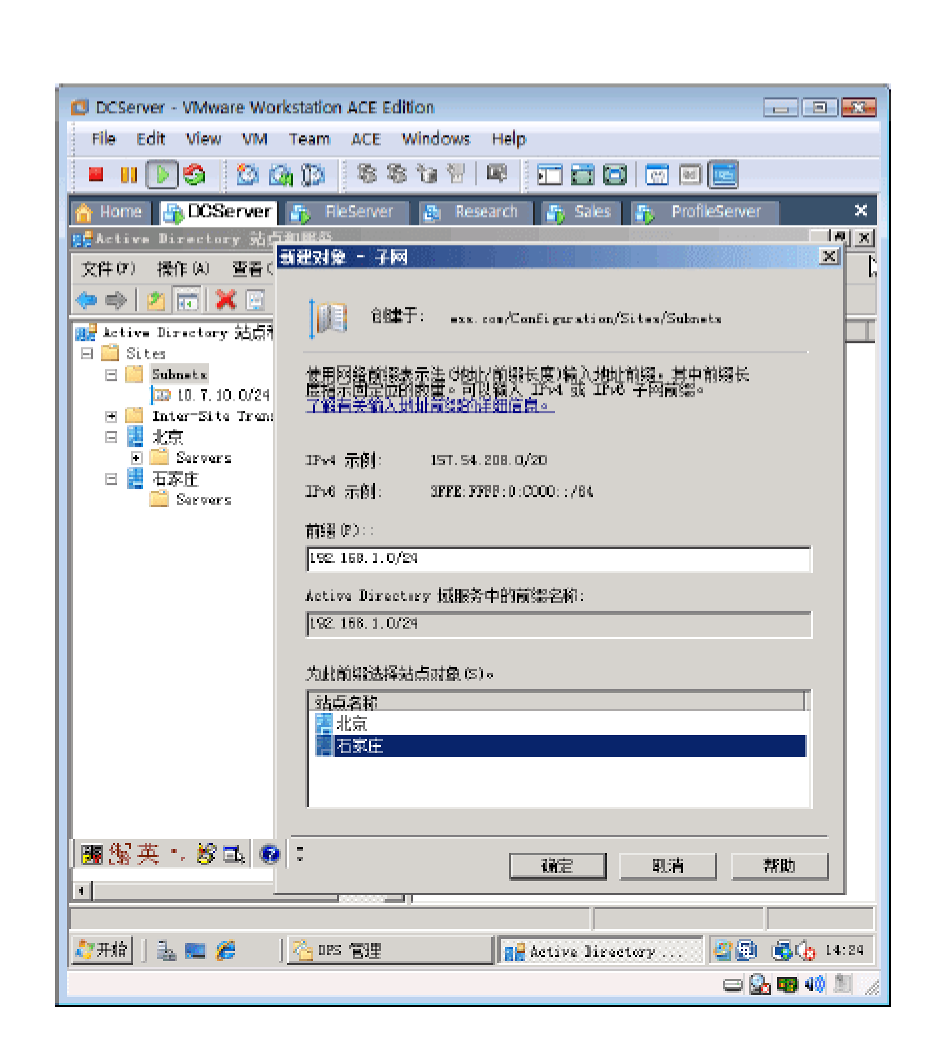


图 7-107　创建石家庄的子网对象

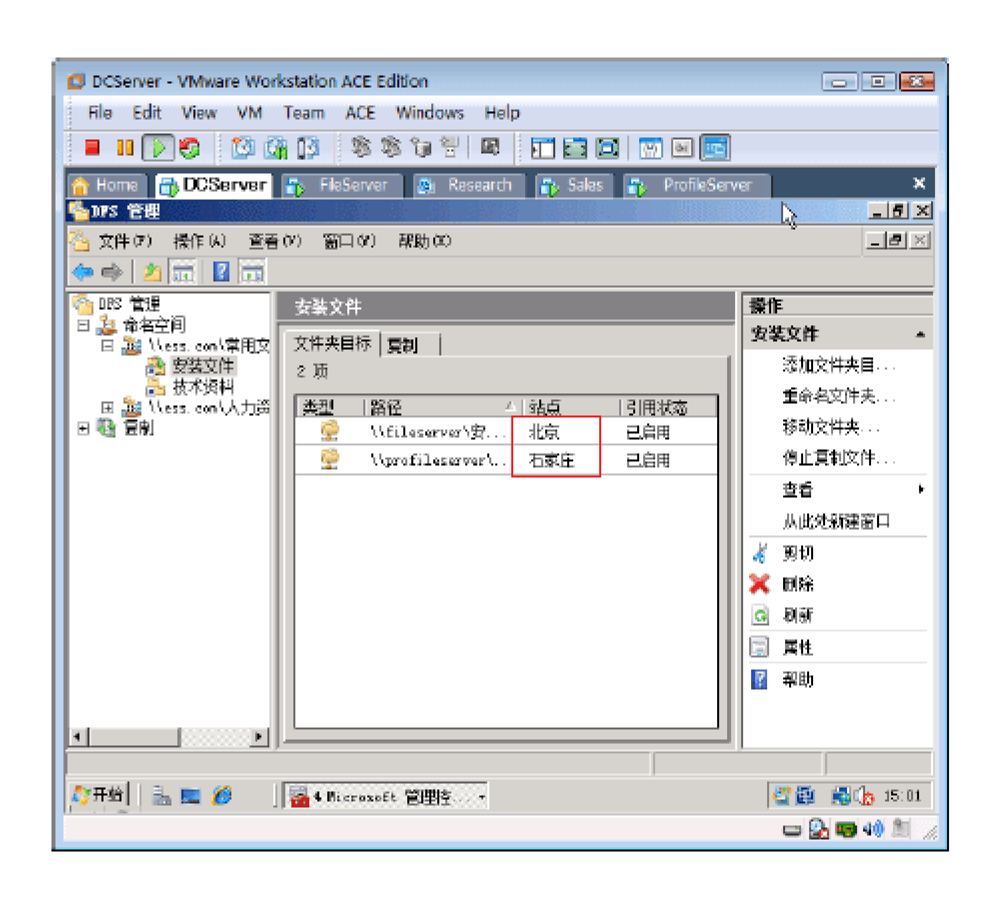


图 7-108　DFS 和活动目录站点

7.3.8　任务 8：测试到 DFS 的连接

前面的操作根据网络的物理结构创建了活动目录站点和子网对象。现在活动目录就可以针对 FileServer 和 ProfileServer 的 IP 地址来断定其所在的活动目录站点。

客户端访问命名空间时，命名空间服务器 DCServer 会根据客户端的 IP 地址，优先将用户定位到与用户在同一站点的文件服务器上。

示例：验证 DFS 连接。

① 以域管理员的用户账户登录 Sales 计算机。

② 将其 IP 地址设置成 10.7.10.56，子网掩码设置成 255.255.255.0，网关设置成 10.7.10.123，DNS 设置成 10.7.10.123。这个地址属于北京站点。

③ 选择“开始”→“运行”命令，在“运行”对话框中输入\\Ess.com ，单击“确定”按钮。

④ 如图 7-109 所示，打开“常用文件”中的“安装文件”。

⑤ 如图 7-110 所示，在 FileServer 计算机上，选择“开始”→“程序”→“管理工具”→“共享和存储管理”命令。

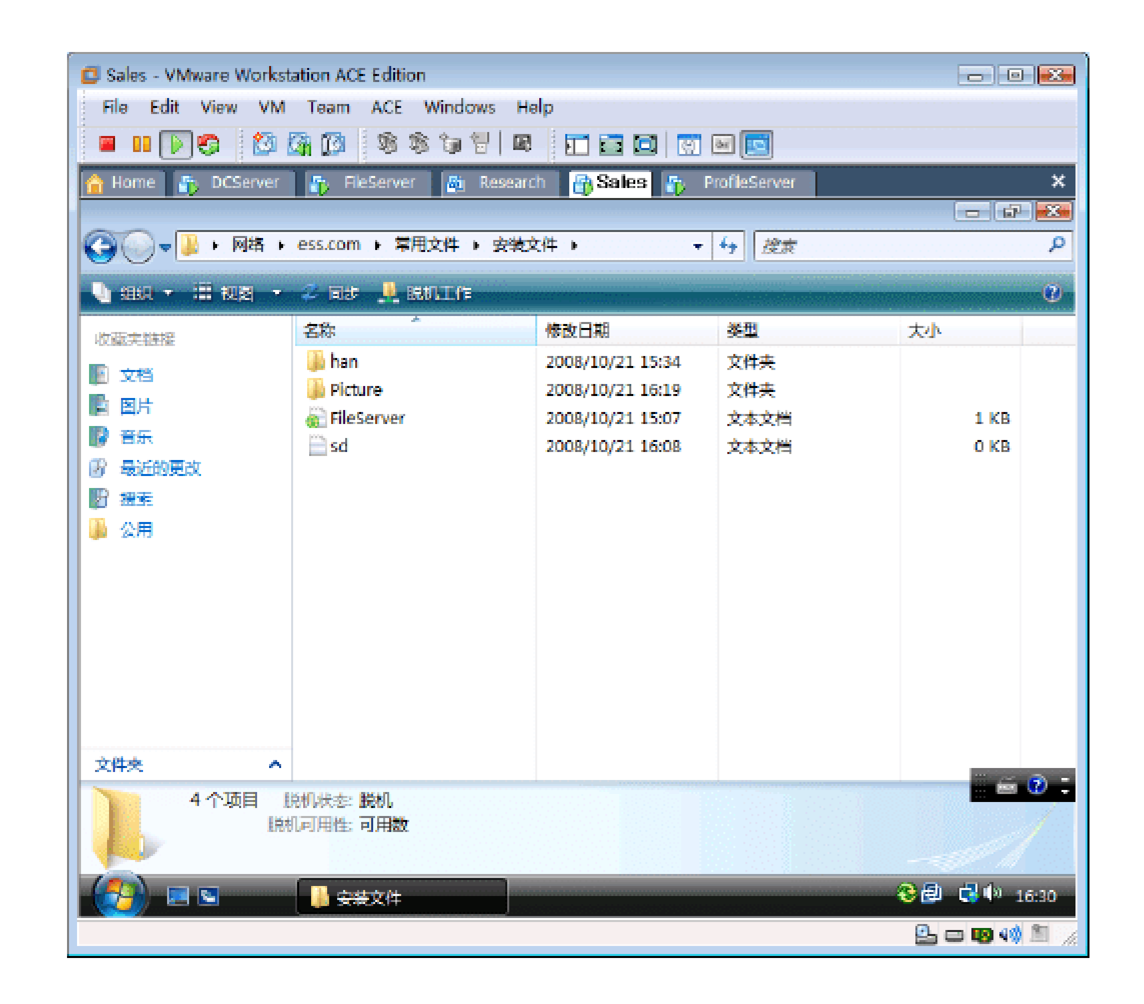


图 7-109 访问名称空间

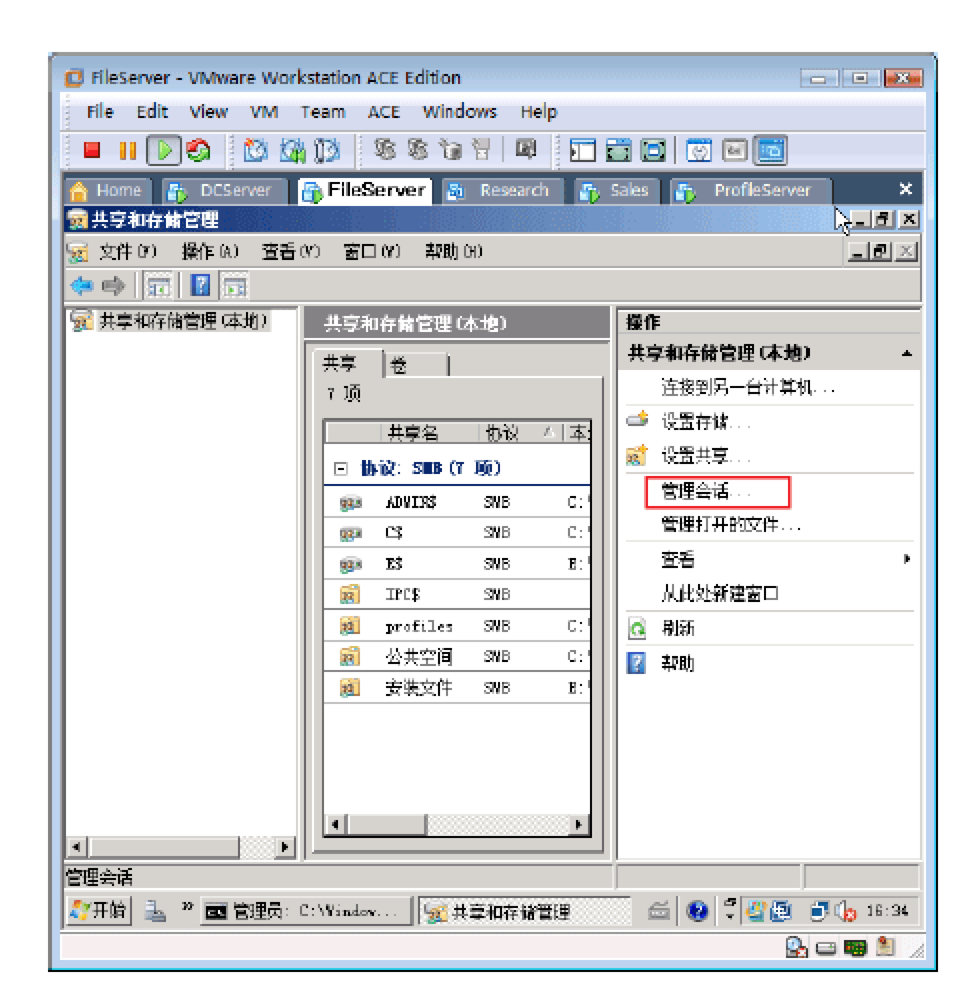


图 7-110 查看会话

⑥ 如图 7-111 所示，可以看到，Sales 计算机访问 DFS 被定位到 FileServer 计算机。FileServer 属于北京站点。

⑦ 将 Sales 计算机的 IP 地址设置成 192.168.1.56，子网掩码为 255.255.255.0，网关设置成 192.168.1.100，DNS 设置成 192.168.1.100。

⑧ 再次打开“\\Ess.com\常用文件”命名空间，单击“安装文件”。

⑨ 如图 7-112 所示，在 ProfileServer 上运行 netstat –n 命令，可以看到 Sales 计算机访问 ProfileServer 共享文件夹建立的会话。访问共享文件夹使用的端口是 TCP 的 445 端口。

⑩ 上面的操作验证了设置活动目录站点和子网对象对用户访问 DFS 的影响。

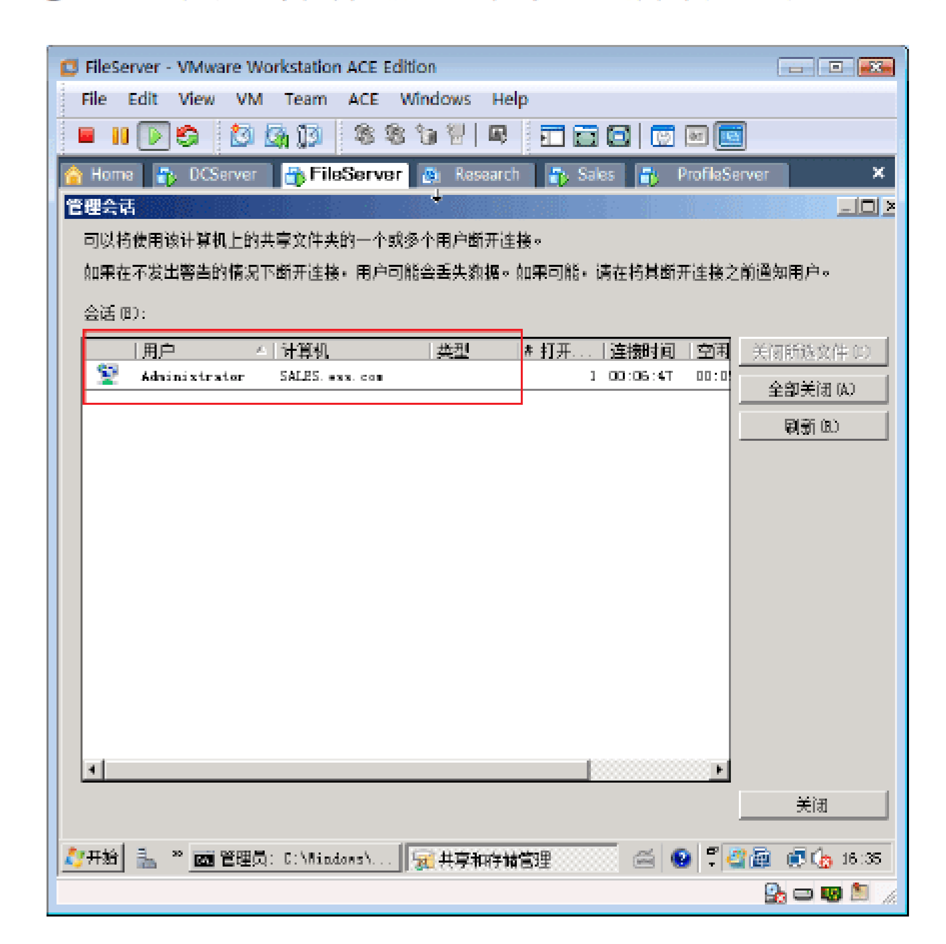


图 7-111 查看访问共享资源的会话

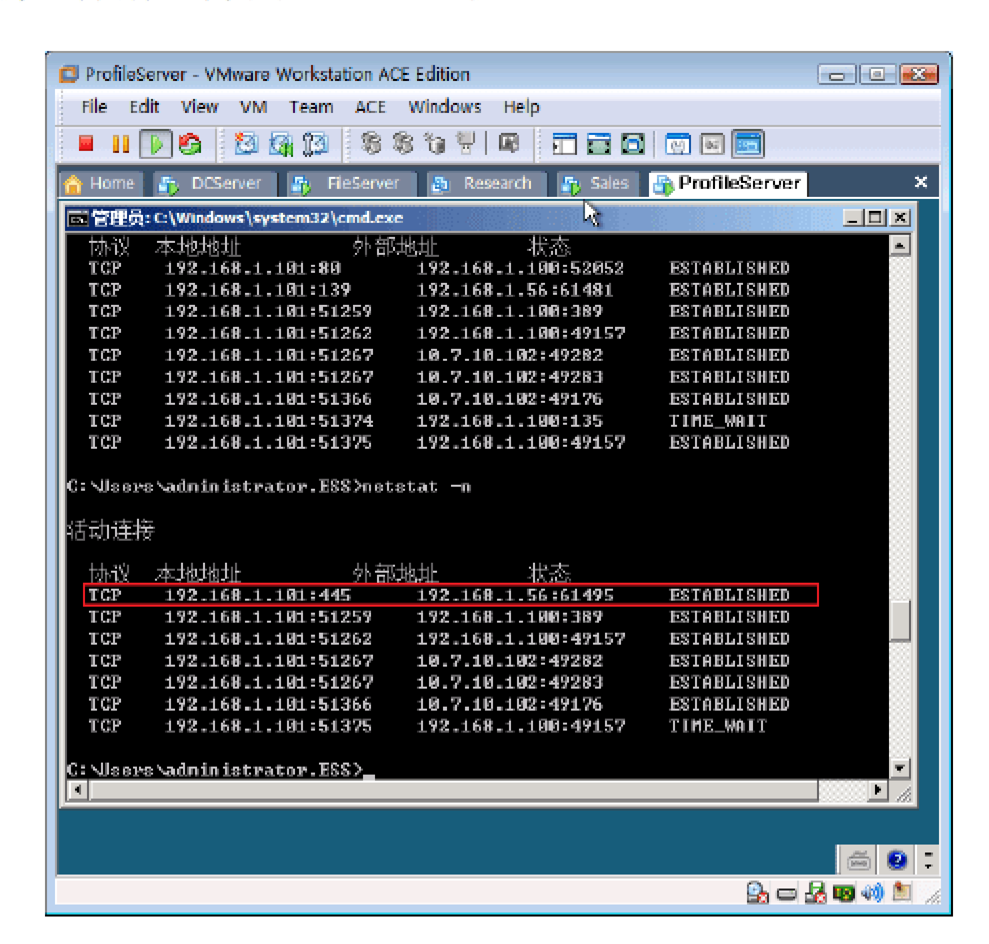


图 7-112 查看会话

7.4 设计分布式文件系统

7.4.1 分布式文件系统的方案和功能

在开始设计之前，最好了解一下设计这些技术所针对的方案以及可以为 Windows Server 2008 中的“DFS 命名空间”和“DFS 复制”配置的基本功能。在复查了方案之后，请记住，“DFS 命名空间”和“DFS 复制”配置之间没有依存关系。两项服务都可以相互独立使用，但是在一起使用时，可以帮助你实现更强大的端到端方案，获得高可用性并实现 WAN 负载平衡。

建议使用分布式文件系统的方案，要实现下列方案，可以将“DFS 命名空间”和“DFS 复制”一起使用。

7.4.2 数据发布

使用 Windows Server 2003 R2 中的“DFS 命名空间”和“DFS 复制”可以在组织范围内(的所有服务器上)给用户发布文档、软件和行业数据。在此方案中，使用“DFS 复制”将数据分发到多台服务器上，同时使用“DFS 命名空间”简化用户对数据的访问并实现高可用性。

图 7-113 说明了如何在分支机构环境中使用“DFS 复制”来复制数据。在分支机构环境中，数据源自中心站点或数据中心的一台或多台中心服务器，并复制到分支机构的服务器上。

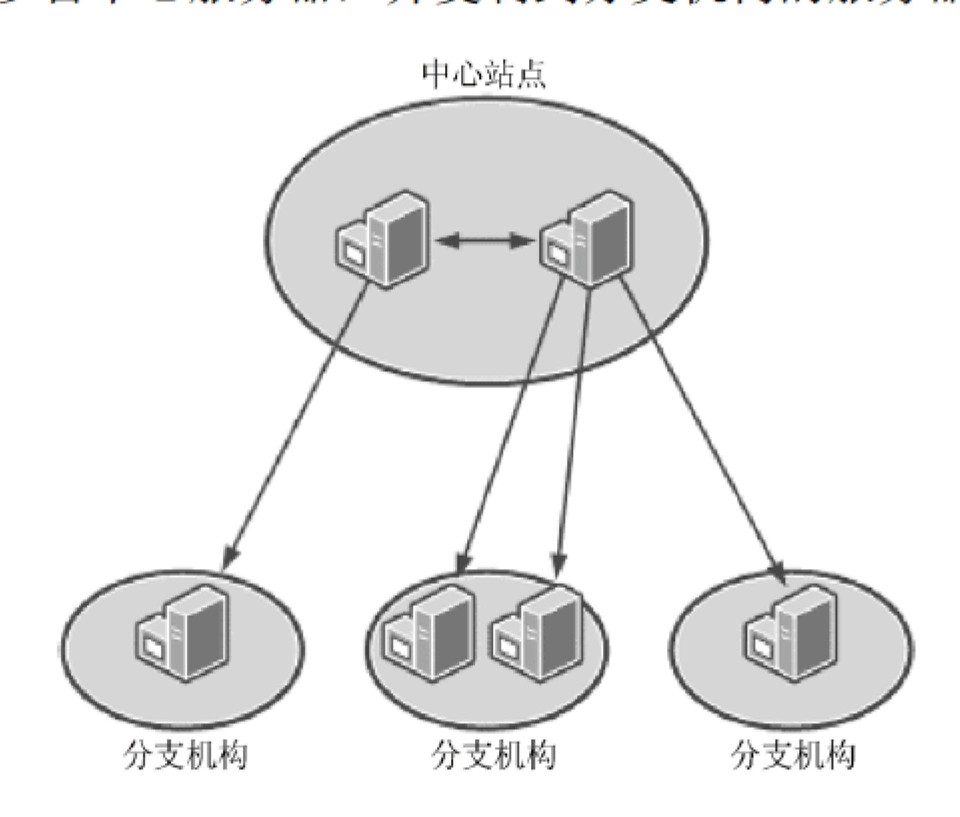


图 7-113 分支机构环境

因为“DFS 复制”是针对慢速 WAN 链路而设计的，所以，它非常适合将文件分发到远程位置的分支机构。远程差分压缩 (RDC) 有助于减少用于复制的网络带宽。“DFS 复制”可以继续复制因 WAN 中断而造成的只复制了一部分的文件。使用“DFS 复制”来分发数据的其他一些好处如下所述。

- 要减少复制源自中心服务器的新文件时所需的 WAN 通信量，可以使用交叉文件 RDC 来确定与需要复制的文件类似的文件。如果文件在中心服务器上而不是在分支服务器上，那么此方法很有用。“DFS 复制”可以使用与需要复制的文件类似的文件的若干部分来代替复制整个文件，从而使通过 WAN 传输的数据量最少。(交叉文件 RDC 的要求如本指南后面的“‘DFS 复制’的功能”中所述)
- 要进一步减少初次复制新数据时所需的复制通信量，可以使用已还原的备份来预安排分支服务器。

“DFS 复制”可以使用 RDC 和交叉文件 RDC 来减少复制任何新文件或已更改文件的若干部分时所需的带宽。

- 可以将复制安排在非工作时间进行，并且可以通过设置带宽限制来控制复制期间使用的带宽。
- 在复制到大量分支服务器时，就中心服务器上的负载来说，“DFS 复制”是非常高效的。原因在于“DFS 复制”只暂存要复制的文件(即准备文件，以便使用 RDC 哈希值进行复制)一次，之后重复使用暂存的文件复制到所有伙伴。

尽管单独使用“DFS 复制”就足以分发数据，但是，使用“DFS 命名空间”可以简化用户对分布式数据的访问并提高数据的可用性。在创建命名空间时，对位于不同服务器上的共享文件夹进行分组，并将其作为虚拟文件夹树提供给用户。命名空间中的任何文件夹都可以由多台服务器托管，每台服务器保留该文件夹中的已发布数据的副本(通过“DFS 复制”保持同步)。浏览命名空间时，用户仅看到一个文件夹，并且不会注意到该文件夹是由多台服务器托管的。对于使用 UNC 路径(例如\\Ess.com\Software\Products\Microsoft\Office)访问数据的用户，基础服务器是完全透明的。

“DFS 命名空间”在以下几种情况时非常适合在分支机构环境中使用。

- 如果客户端计算机自己的 Active Directory 站点中存在服务器，那么客户端计算机将先访问这些服务器。可以选择限制客户端计算机，使其仅访问自己站点中的服务器。
- 如果某台服务器出现故障，那么客户端可以将故障转移到同一个站点中的另一台服务器上(如果存在另一台服务器)。如果同一站点中没有其他服务器，客户端可以将故障转移到连接成本最低的服务器上(根据“Active Directory 站点和服务”管理单元中的定义)。
- 在本地服务器恢复之后，可以配置命名空间，以便客户端故障回复到本地服务器。(注意，此功能要求在客户端上安装热修补程序)

图 7-114 示出了“DFS 命名空间”的两项功能——客户端故障转移和目标优先级，因为这两项功能可以在拥有中心站点和两个分支机构的环境中使用。假定在正常操作期间，分支机构的客户端使用命名空间服务器中的引用来访问本地服务器。如果本地分支服务器出现故障，并且配置了目标优先级，可能会进行故障转移，如下所述。

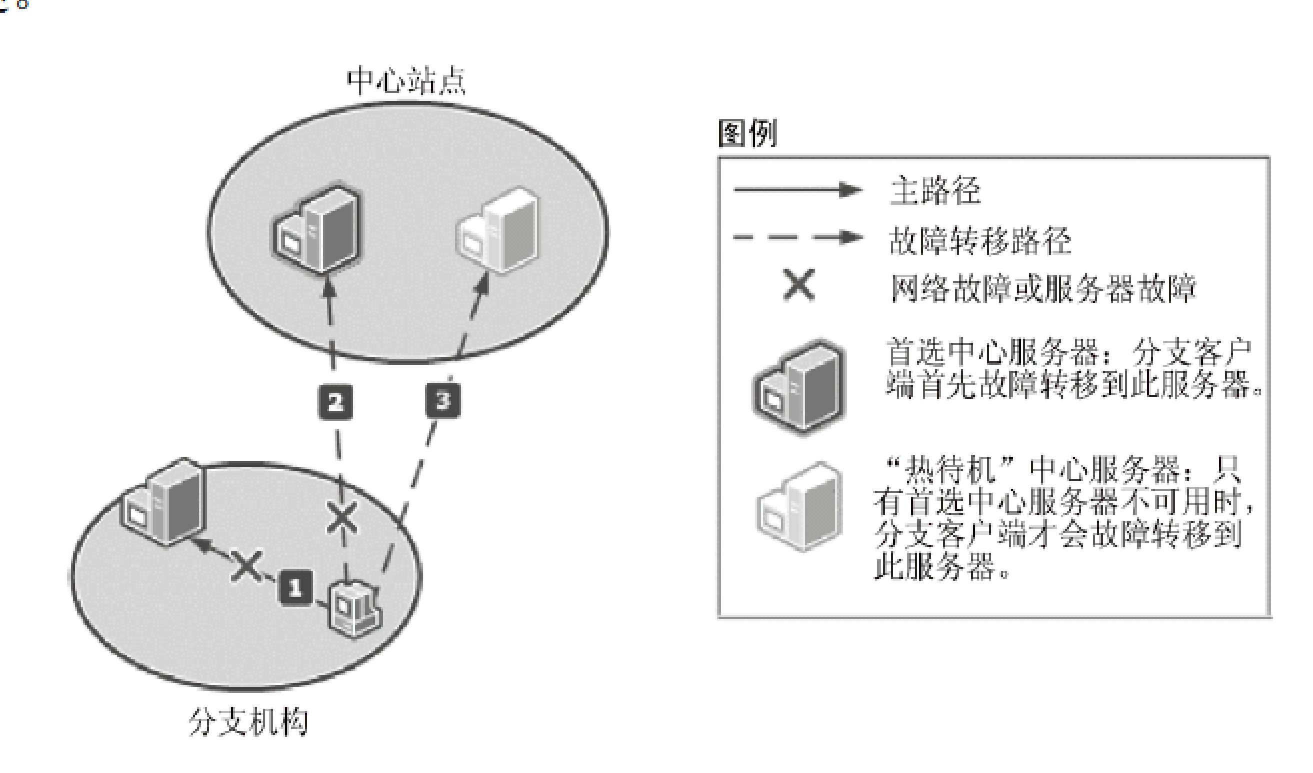


图 7-114 故障转移和目标优先级

- 分支站点中的客户端尝试访问本地服务器上的某个文件夹目标，但是该服务器不可用。
- 客户端尝试将故障转移到中心站点的两台服务器中的一台。如果希望客户端始终将故障转移到中心站点的特定服务器，那么可以将中心服务器的目标优先级配置为成本相等的目标中的第一项。客户端先尝试故障转移到这台首选的中心服务器。

- 如果首选的中心服务器不可用，客户端将尝试访问另一台中心服务器(可能是中心站点的“热待机”服务器)。可以将此中心服务器的优先级配置为成本相等的所有目标中的最后选项。



注意：如上文所述，可以通过配置命名空间，使分支机构中的客户端可以在分支服务器恢复后，故障回复到分支服务器。

7.4.3　数据收集

数据收集方案有助于避免在分支机构中使用磁带备份。要实现此目标，使用“DFS 复制”将数据从分支机构的某台服务器复制到中心站点或数据中心的某台服务器上。中心站点的管理员可以使用备份软件从中心服务器备份分支服务器的数据，以避免让最终用户在没有配备受训 IT 人员的分支机构执行备份，因为这个过程经常容易出错。集中备份还有助于降低硬件成本和运营成本。图 7-115 为说明此方案的示意图。

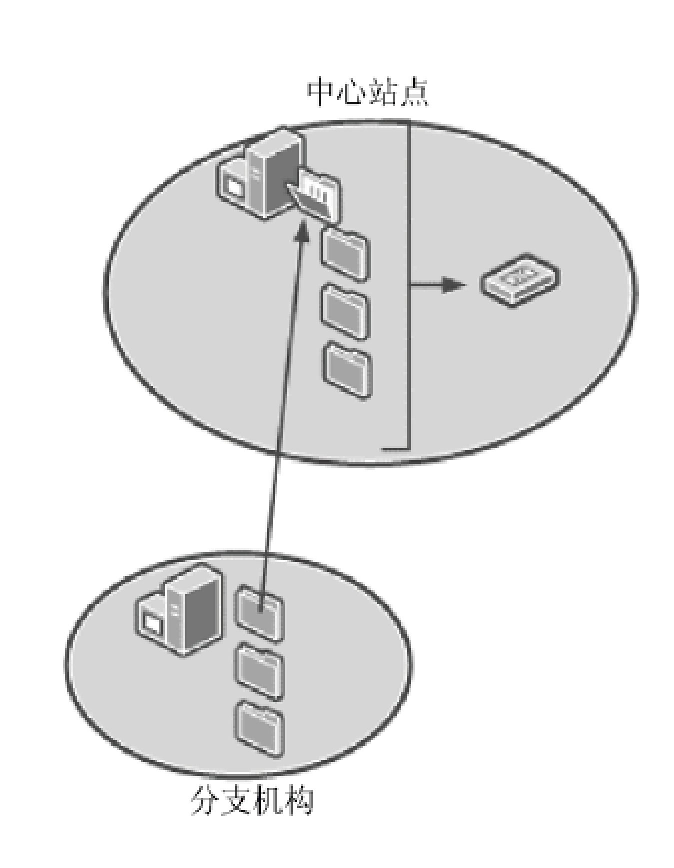


图 7-115　数据收集

通过 RDC，“DFS 复制”仅复制两台服务器之间不同的内容(或更改)，因此，可以使复制期间使用的带宽最少。对于与中心机构建立低带宽 WAN 连接的分支机构，这一点非常重要。此外，还可以使用带宽限制来控制复制期间所使用的带宽，使用户可以更好地控制 WAN 通信量。

将“DFS 复制”与“DFS 命名空间”组合使用，可以通过配置命名空间，使分支客户端始终连接到分支服务器上。如果分支服务器不可用，那么分支客户端将故障转移到中心服务器。如果配置了客户端故障回复，那么分支客户端将在分支服务器恢复之后故障回复到分支服务器。



注意：客户端故障回复要求在客户端上安装热修补程序。

图 7-116 给出了客户端故障回复的过程。下面将详细地介绍该过程。

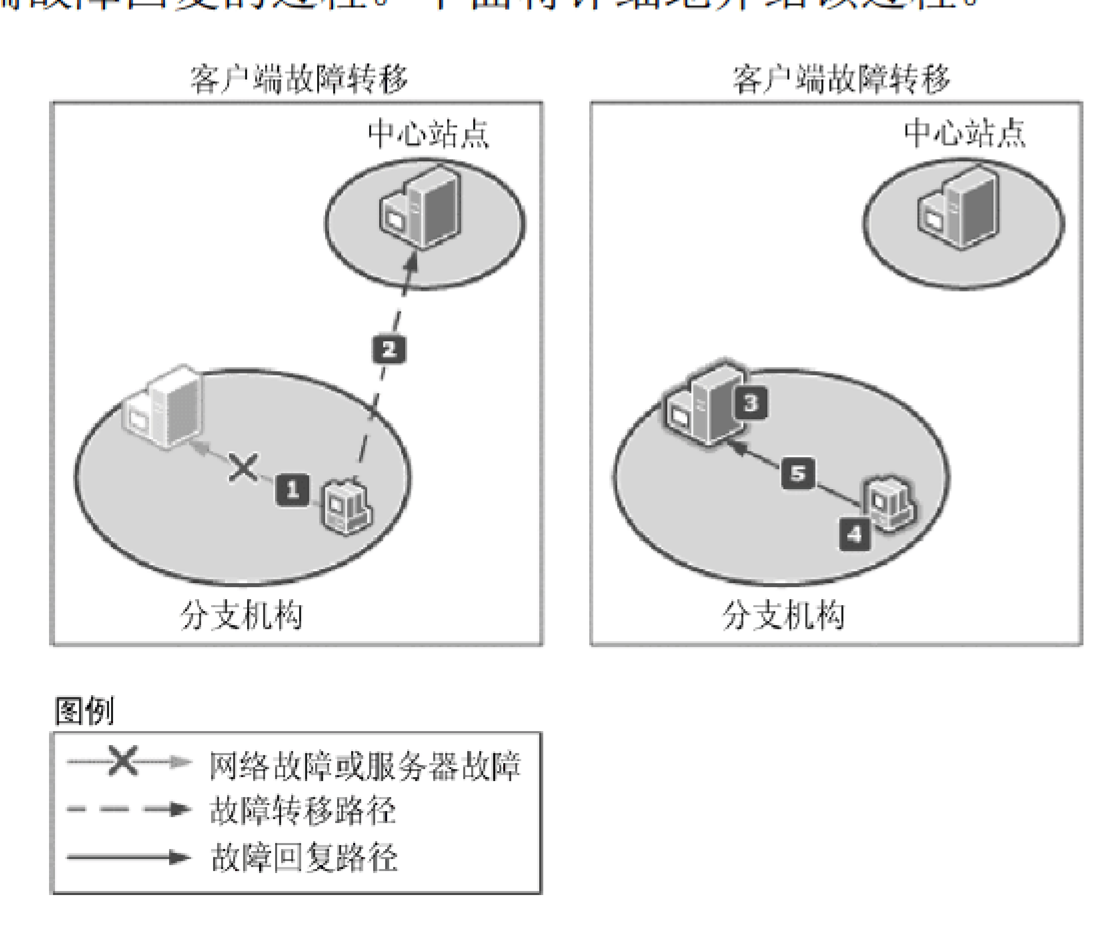


图 7-116　故障回复过程

在图 7-116 中，客户端故障转移和故障回复的工作过程如下所述。

① 本地分支服务器出现故障或因为网络问题导致不可用。

② 客户端故障转移到中心站点的服务器。在客户端的引用过期、重新启动客户端计算机或清除客户端的引用缓存之前，客户端将一直访问此服务器。(引用是一个排序的服务器列表，这些服务器托管与命名空间中的某个文件夹关联的共享文件夹)

③ 分支服务器恢复。

④ 在引用过期、重新启动客户端或清除客户端的引用缓存之后，客户端将请求新的引用。(此步骤与分支服务器的恢复无关)

⑤ 在收到新引用之后，客户端将故障回复到已恢复的分支服务器。



提示：关于活动目录站点设计，请参照本系列《掌控 Windows Server 2008 活动目录》一书。

7.4.4 设计命名空间

下面介绍设计命名空间层次结构，选择引用排序方法和目标优先级，以及配置客户端故障回复。

命名空间层次结构

要设计命名空间层次结构，请选择命名空间的名称(也称为根路径名称)，将出现根路径下的文件夹的名称以及文件夹的层次结构。根路径名称和文件夹名称不仅应反映组织的需要，还应反映用户计划分发的数据类型。

应根据下列基本准则来选择命名空间名称和文件夹名称。

- 命名空间名称在服务器名称或域名的上面，位于逻辑命名空间层次结构的顶部。此级别的名称需要标准化和有意义，域中有多个命名空间时尤其如此，因为用户是通过命名空间名称进入命名空间的。
- 命名空间的文件夹名称和层次结构对用户来说必须尽可能清楚，以便用户不会进入错误的路径而不得不按原路径返回。要尽可能减少用户进入错误路径的次数，并避免用户在与不必要的目标建立连接时可能遇到的延迟，应为命名空间中的文件夹设计有意义的命名方案。
- 命名空间不必适应文件系统上的本地文件组织；而应适应组织的业务需要。
- 命名空间应与地理位置无关。例如，即使华盛顿的用户只看到应用程序的一个子集，创建命名空间路径(例如 \\Contoso.com\Washington\Applications)也不会起任何作用。禁用给定服务器上已复制文件夹的成员身份，以便在发布时控制此准则。

如果计划创建包含大量文件夹的命名空间，那么命名方案和层次结构尤其重要，可以使用户不必扫描长长的文件夹列表来查找所需的文件夹。使用没有目标(本质上是命名空间子文件夹)的文件夹可以帮助构建更深的层次结构，使用户可以从少量的顶级文件夹中作出选择。

要减少命名空间层次并减少用户在浏览该命名空间时看到的文件夹数量，应考虑使用基于访问权限的文件夹枚举。该功能在 Windows Server 2003 SP1 中初次引用，可以对没有访问权限的用户隐藏文件夹。

7.4.5 引用排序和目标优先级

在客户端计算机尝试访问命名空间时，域控制器或命名空间服务器将提供对该客户端的引用。引用包

含按照当前配置的排序方法和目标优先级进行排序的目标服务器列表。客户端访问命名空间根路径或命名空间中的某个文件夹时，将尝试访问引用顶部的第一个目标；如果前面的目标不可用，客户端将转到下一个目标。

默认情况下，将选择最低成本排序方法，如图 7-117 所示。在此方法中，目标如下所述进行排序(假定没有目标优先级设置覆盖此方法的默认行为)。

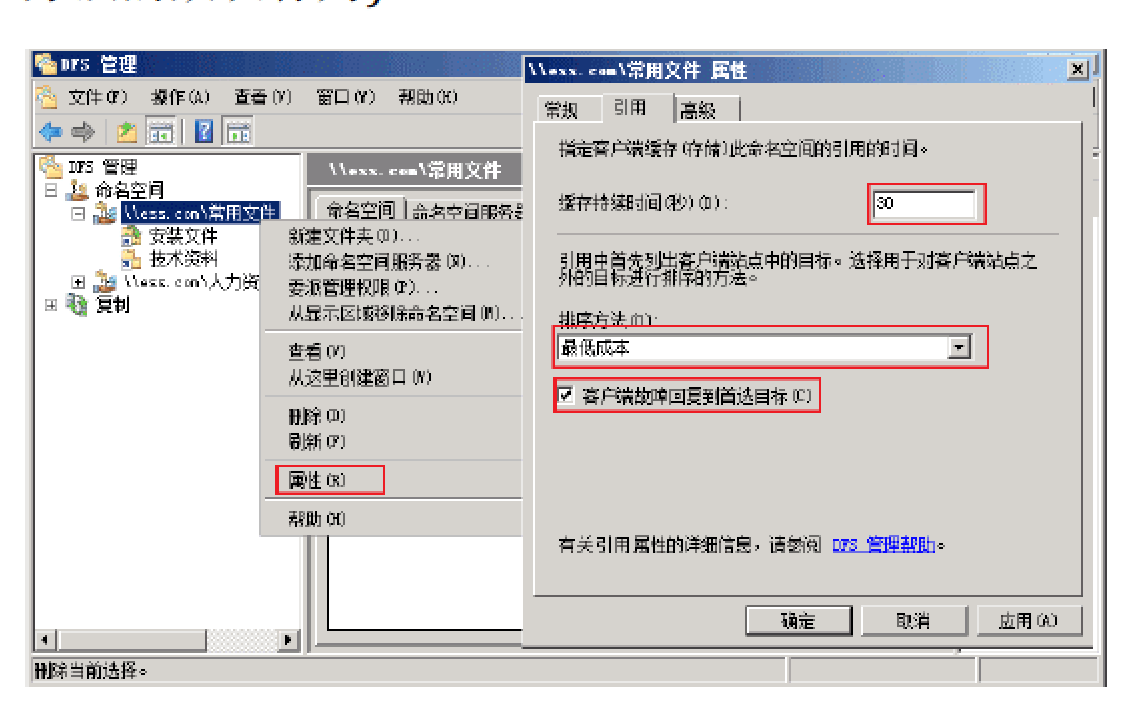


图 7-117　设置引用规则

- 与客户端处于同一活动目录站点的目标按照随机顺序列在引用的顶部。
- 客户端站点之外的目标按照最低成本到最高成本的顺序列出。成本相同的引用组合在一起，每个组中的目标按照随机顺序列出。

如果希望禁止分支客户端故障转移到其他分支站点中的分支服务器，那么为每个包含目标的文件夹选择“排除客户端站点之外的目标”排序方法，然后通过选择“所有目标中的最后一项”目标优先级，为每个中心服务器的文件夹目标设置目标优先级。选择这两个选项的结果如下。

- “排除客户端站点之外的目标”设置确保只有客户端站点内的目标将加入引用。
- “所有目标中的最后一项”设置通过将中心服务器加入引用，覆盖引用排序方法，即使中心服务器不在客户端站点中也是如此。(如果多台中心服务器作为给定文件夹的目标使用，那么这些中心服务器将在引用中最后出现，在其他目标之后按照最低成本的顺序进行排序)

如果计划使用最低成本引用排序和目标优先级，那么要注意，域控制器和命名空间服务器必须运行本指南前面的“‘DFS 命名空间’的要求”中所述的操作系统。如果域控制器或命名空间服务器运行的是 Windows 2000 Server，那么无法根据成本或优先级提供引用。这些服务器中的引用将使用随机引用排序，如下所述(假定没有目标优先级设置覆盖此方法的默认行为)。

- 与客户端处于同一站点的目标按照随机顺序列在引用的顶部。
- 客户端站点之外的目标按照随机顺序列出。如果没有处于同一站点的目标服务器，那么客户端计算机将引用到随机目标服务器，与连接的成本或目标的距离无关。

只有在 Active Directory 中启用了“为所有站点链接搭桥”选项，最低成本排序方法才适用于所有目标。(此选项以及站点链接成本在“Active Directory 站点和服务”管理单元中提供)运行 Windows Server 2008 的站点间拓扑生成器需要选中“为所有站点链接搭桥”复选框，才能生成站点间成本矩阵，以满足“分布式文件系统”服务的站点成本计算功能的需要。

如果禁用此选项，那么“分布式文件系统”服务仅计算从分支位置到其他具有直接站点链接的站点的成本。所有没有直接站点链接的站点将使用可能的最大成本。例如，假定分支站点与三个区域数据中心之

间的拓扑如图 7-118 所示进行配置。

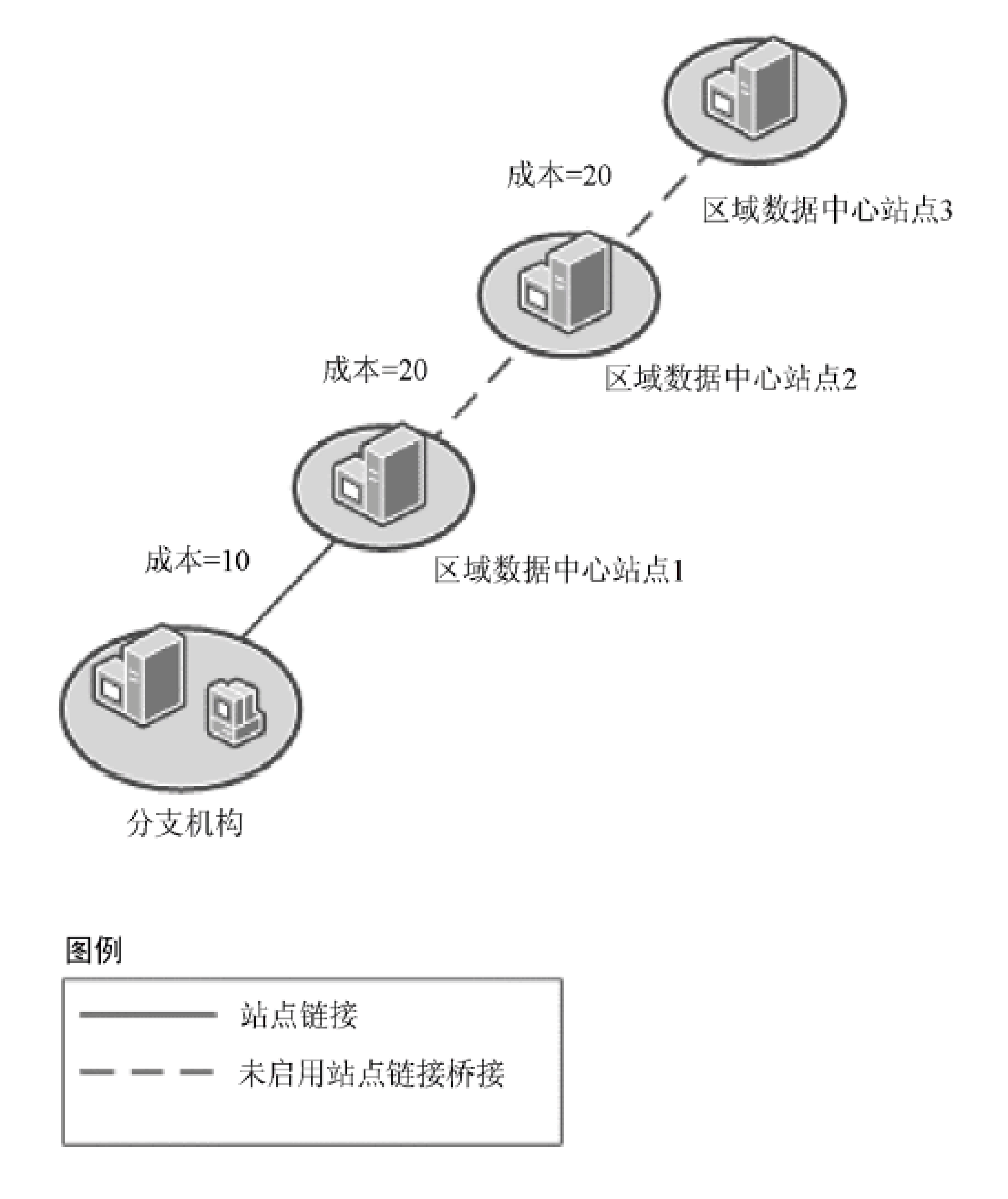


图 7-118 站点间链接成本

如图 7-118 所示，分支站点与区域数据中心站点 1 之间具有站点链接。分支站点与其他区域数据中心之间没有配置站点链接。分支站点中的客户端收到引用时，目标将按如下所述进行排序。

- 分支站点中的服务器。(因为服务器与客户端处于同一站点，所以，其成本为 0)
- 区域数据中心站点 1 中的服务器。(因为此数据中心与分支机构之间存在站点链接，所以，此服务器第二个列出)
- 按照随机顺序列出接下来的两个数据中心。(因为“分布式文件系统”服务无法确定其站点成本，所以，这两台服务器按照随机顺序列出)

如果启用了“为所有站点链接搭桥”选项，那么引用中的服务器将按照以下顺序列出。

- 分支站点中的服务器。
- 区域数据中心站点 1 中的服务器。(成本 = 10)
- 区域数据中心站点 2 中的服务器。(成本 = 30)
- 区域数据中心站点 3 中的服务器。(成本 = 50)

7.4.6 客户端故障回复

“DFS 命名空间”中的客户端故障转移是在一台服务器发生故障或从命名空间中删除之后，客户端尝试访问引用中另一台服务器的过程。如果客户端故障转移到中心服务器并在分支服务器恢复之后仍继续访问中心服务器，可能不需要执行此行为。如图 7-119 所示，如果希望在本地服务器恢复之后，客户端故障回复到首选的本地服务器，那么需要为根路径选中“客户端故障回复到首选目标”复选框。如果为根路径选择了此复选框，那么包含目标的文件夹也将使用故障回复。

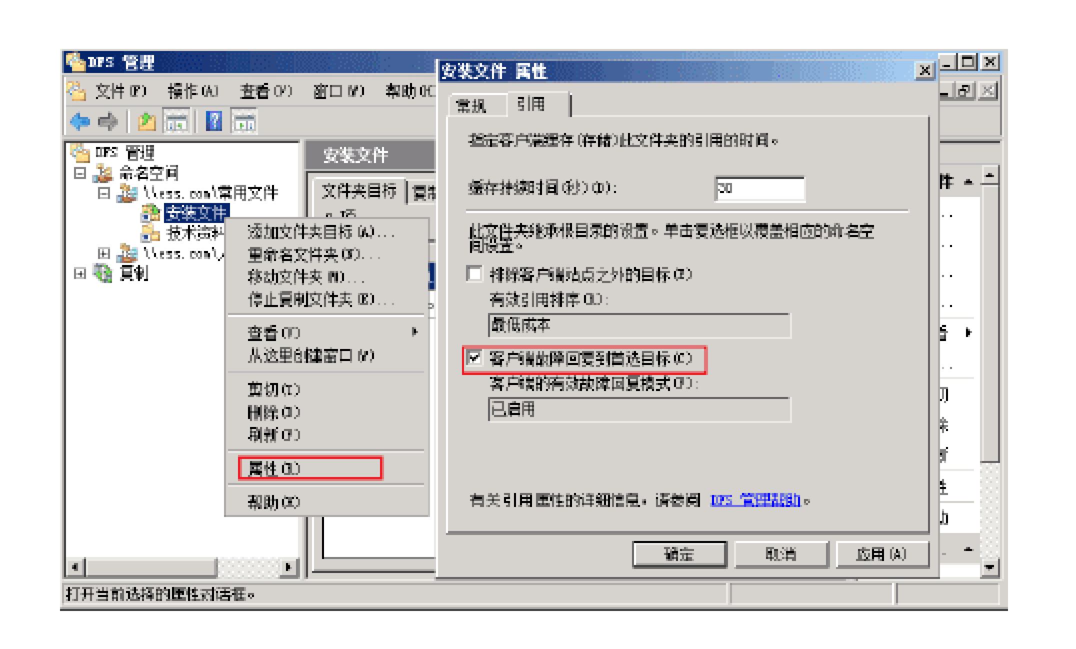


图 7-119　客户端故障回复设置

7.5　脱机使用文件夹

7.5.1　了解脱机文件

如果用户需要访问存储在网络上共享文件夹中的重要文件，但是由于网络连接不可用而无法访问，则应该了解脱机文件的需求。使用脱机文件，即使在网络副本不可用时，也可以访问存储在共享网络文件夹中的文件。可以通过选择要在脱机时可用的网络文件来执行此操作，这会自动在计算机上创建网络文件的副本。这些存储在计算机上的网络文件副本称为脱机文件。Windows 会在网络版本不可用时自动为用户同步脱机文件并打开它们。

可以在连接到存储网络文件的计算机时访问网络文件，如图 7-120 所示。

可以在无法连接到存储网络文件的计算机时访问网络文件的本地副本，如图 7-121 所示。

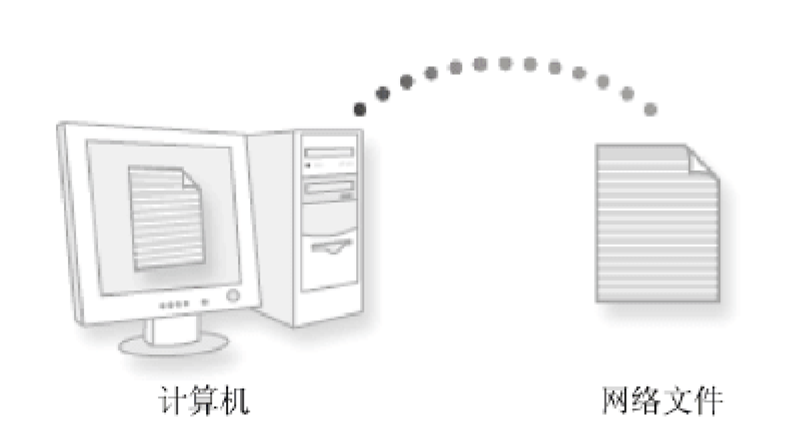


图 7-120　连接网络同步文件

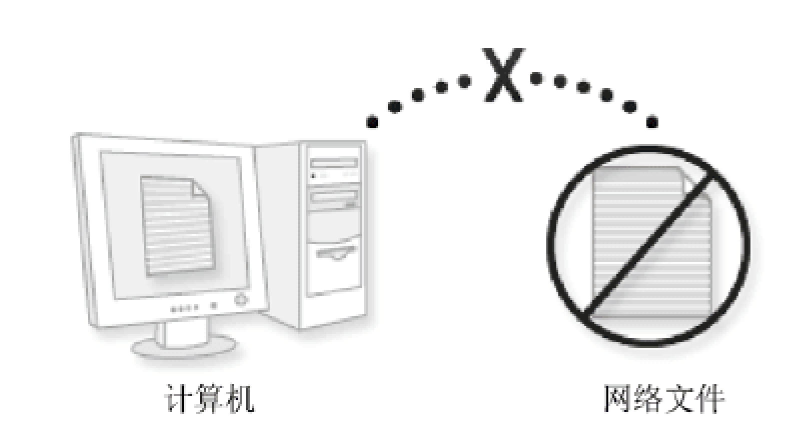


图 7-121　断开网络脱机使用

7.5.2　使用脱机文件的原因

脱机文件对于使用共享网络文件夹存储文件的用户有以下几个优点。

- 保护用户不出现网络问题。使用脱机文件时，不管是网络关闭或是所访问的网络文件夹不可用，这都没有关系。如果发生上述两种情况，Windows 会自动开始访问存储在计算机上的文件的脱机副本，而不是访问网络文件夹中的文件，且用户可以继续进行处理而不被中断。
- 离开网络时使用文件。从网络断开连接时，通常会失去访问存储在网络上的任何文件的能力。但是使用脱机文件，可以从网络断开连接，并仍具有设置为脱机可用的所有网络文件的副本。这在携带移动 PC 旅行时特别有用。
- 与网络文件轻松同步。任何时候用户想和网络文件夹中的最新版本的文件同步时，只需单击一下

按钮，脱机文件就可以执行此操作。

- 在较慢连接上工作时提高效率。连接到连接较慢的网络时，使用共享网络文件夹中文件的效率很低，而且很慢。通过随时轻松地切换到使用网络文件的脱机副本，脱机文件使用户免除了此问题的困扰。

7.5.3 保持脱机文件同步

选择要设置为脱机可用的网络文件或文件夹时，Windows 会自动在计算机上创建该文件或文件夹的副本。任何时候重新连接到该网络文件夹时，Windows 都会同步计算机和网络文件夹之间的文件。还可以随时手动同步这些文件。

这就是保持脱机文件同步所要了解的内容。但是，对于一些好奇的人，还有其他一些详细信息。

- 如果用户脱机工作，并从网络文件夹对脱机文件进行更改，则 Windows 会在下次连接到网络文件夹时自动同步对文件进行的更改。
- 如果用户脱机工作时其他人对共享网络文件夹中的文件进行更改，则 Windows 会在下次连接到该网络文件夹时将这些更改与用户计算机上的脱机文件同步。如果上次连接到网络文件夹以后用户也更改了这些文件，则会发生同步冲突，Windows 会询问用户想要保留哪个版本。
- 如果 Windows 尝试在计算机和网络文件夹之间同步脱机文件时遇到问题(例如，如果尝试同步的网络文件夹不可用)，则会发生同步错误。有关详细信息，请参阅了解同步错误和警告。

7.5.4 示例：脱机使用文件夹

Vista 不需要安装任何功能就支持脱机使用文件夹，Windows Server 2008 需要安装“桌面体验”功能，才支持脱机使用共享的文件夹。

在 Sales 计算机脱机使用 FileServer 计算机上的“安装文件”。

① 在 FileServer 计算机上右击共享的“安装文件”，从弹出的快捷菜单中选择“属性”命令，如图 7-122 所示，在“文件夹 属性”对话框的“共享”选项卡中，单击“高级共享”按钮。

② 如图 7-122 所示，在“高级共享”对话框中单击“缓存”按钮。

③ 如图 7-123 所示，在“脱机设置”对话框中选中“只有用户指定的文件和程序才能在脱机状态下可用”单选按钮，单击“确定”按钮。

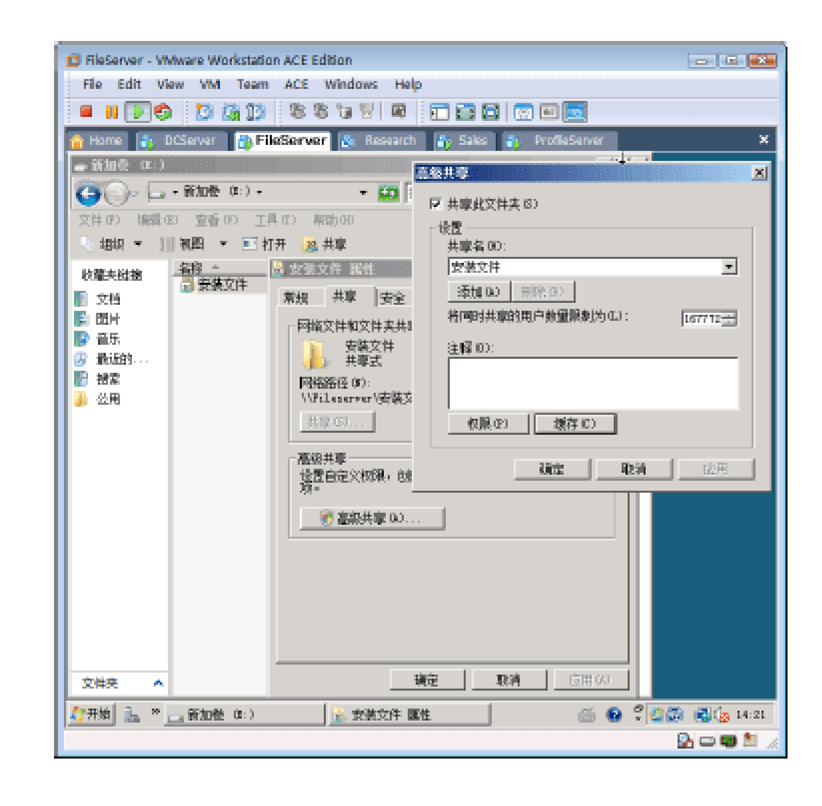


图 7-122 配置共享文件夹

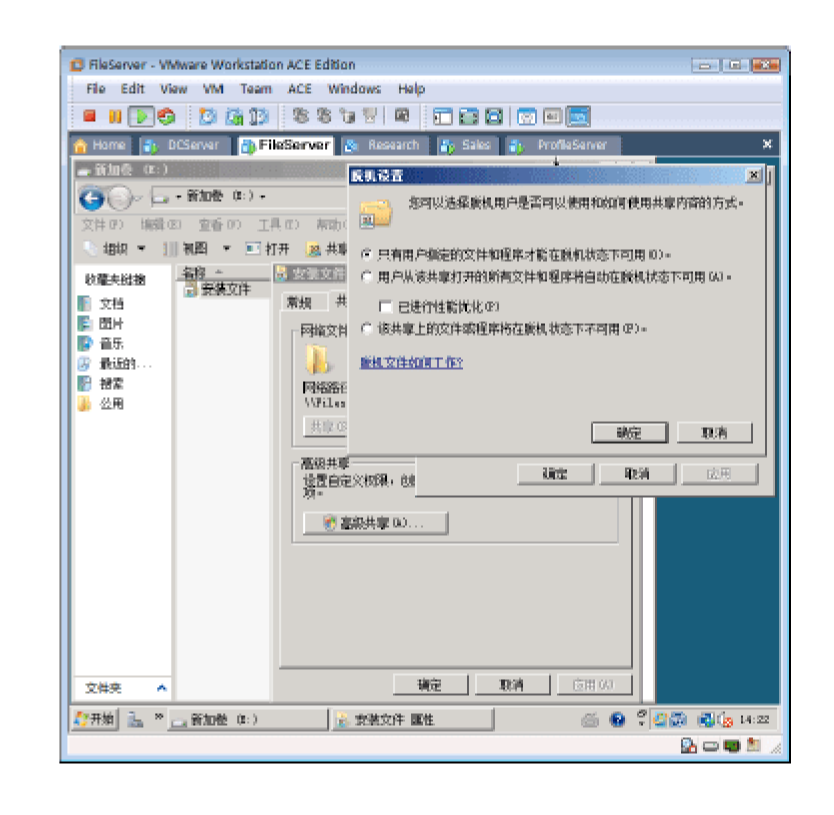


图 7-123 共享文件夹允许缓存

④ 如图 7-124 所示，在 Sales 计算机上。选择“开始”→“设置”→“控制面板”→“脱机文件”命令。

⑤ 如图 7-125 所示，默认 Vista 操作系统已经开启了脱机文件夹，Windows Server 2008 操作系统默认禁用脱机文件。





图 7-124　配置脱机文件

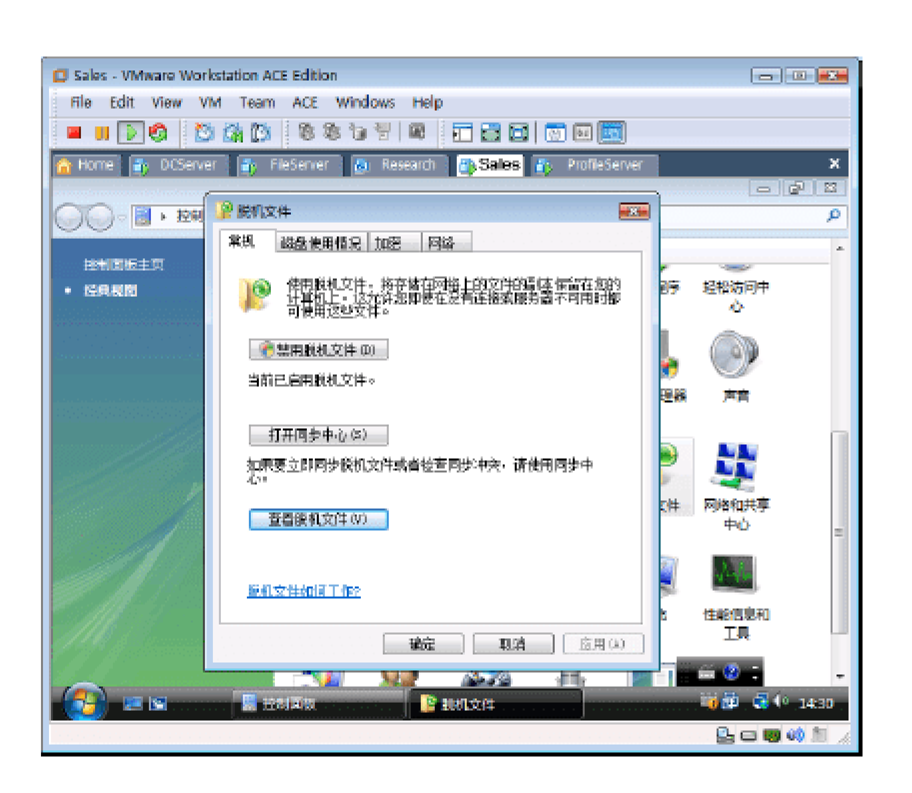


图 7-125　默认启用脱机文件

⑥ 如图 7-126 所示，打开 FileServer 服务器上共享的文件夹，右击 FileServer.txt，从弹出的快捷菜单中选择“始终脱机可用”命令。

⑦ 如图 7-127 所示，可以看到脱机的文件，图标已经变成 FileServer 。

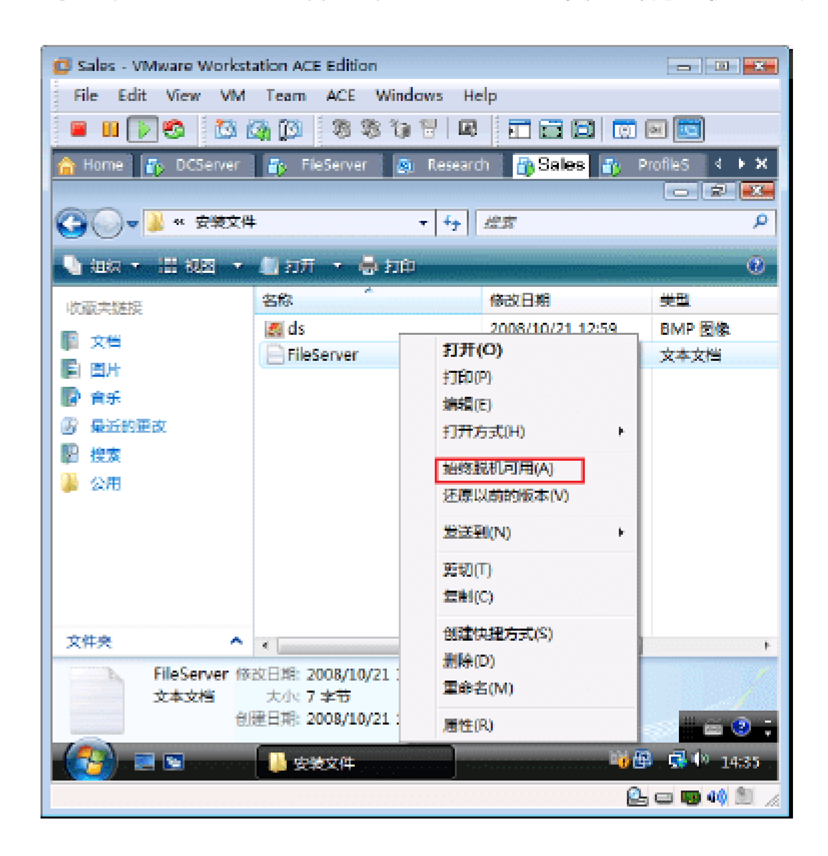


图 7-126　脱机使用文件

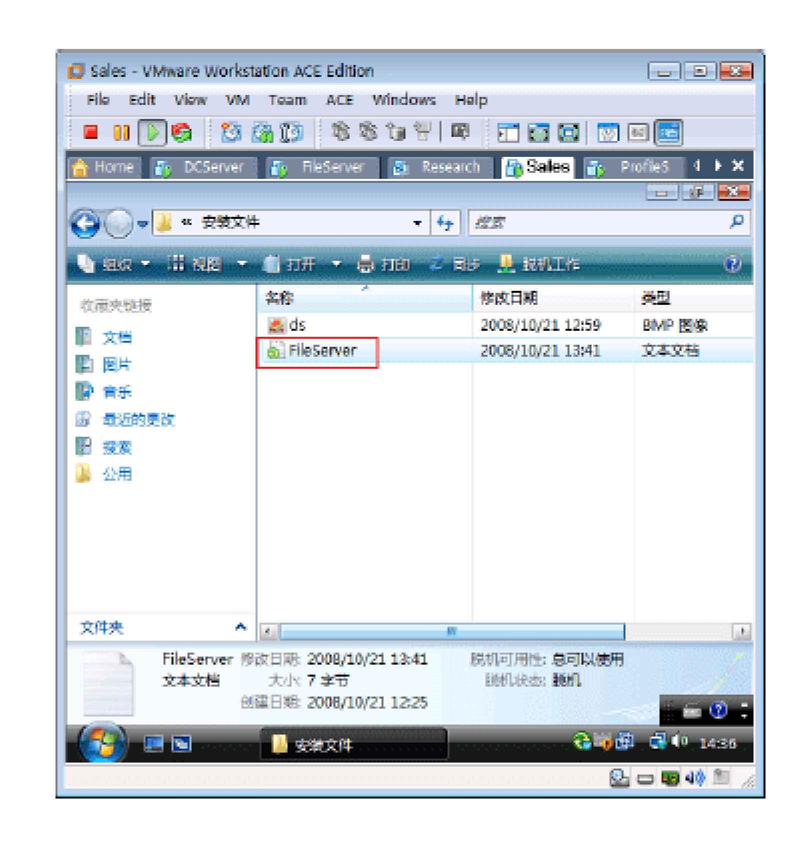


图 7-127　脱机的文件图标

⑧ 断开 Sales 的网络连接。现在服务器不可访问。

⑨ 单击工具栏中的“同步中心”按钮。

⑩ 如图 7-128 所示，单击“脱机文件”按钮。

⑪ 如图 7-129 所示，打开常用文件夹中的安装文件，可以看到 FileServer.txt 文件夹，双击可以将其打开。编辑后保存。

⑫ 用户也可以如同网络连接正常时一样的方式访问脱机文件，如图 7-130 所示，在“运行”对话框中输入“\\Ess.com”，按 Enter 键，可以看到“常用文件”中的 FileServer.txt 文件可访问。

⑬ 如图 7-131 所示，将 Sales 计算机的网络连接，右击 FileServer.txt，从弹出的快捷菜单中选择“同步”命令。

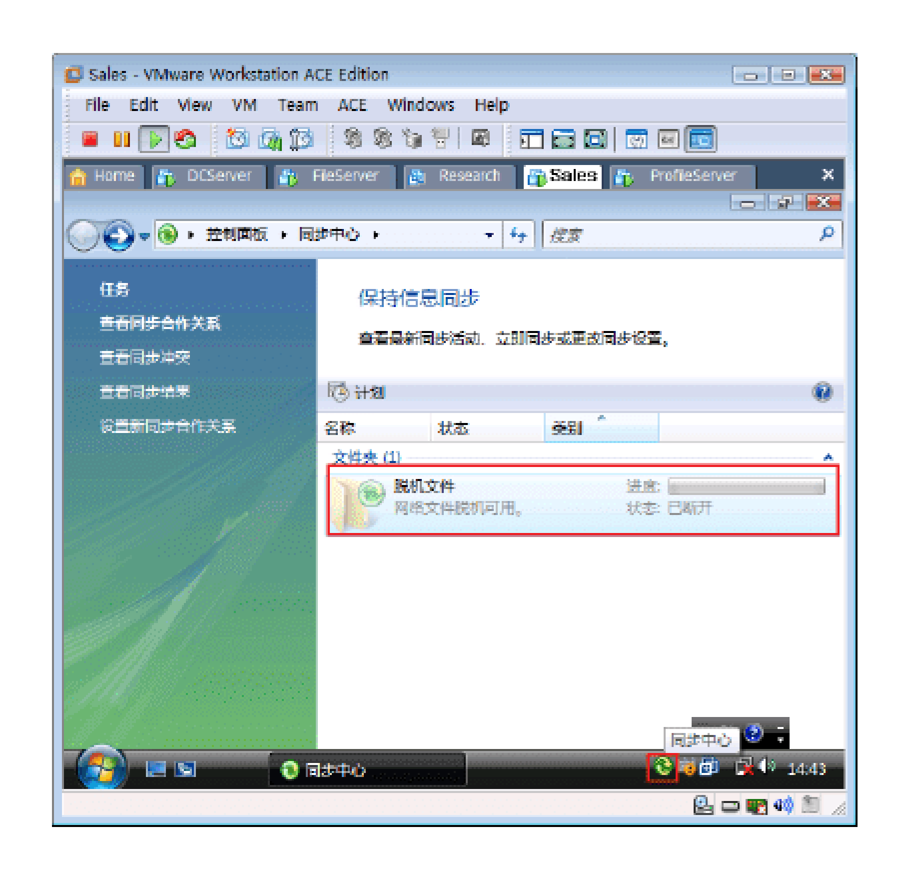


图 7-128　断开网络打开脱机文件

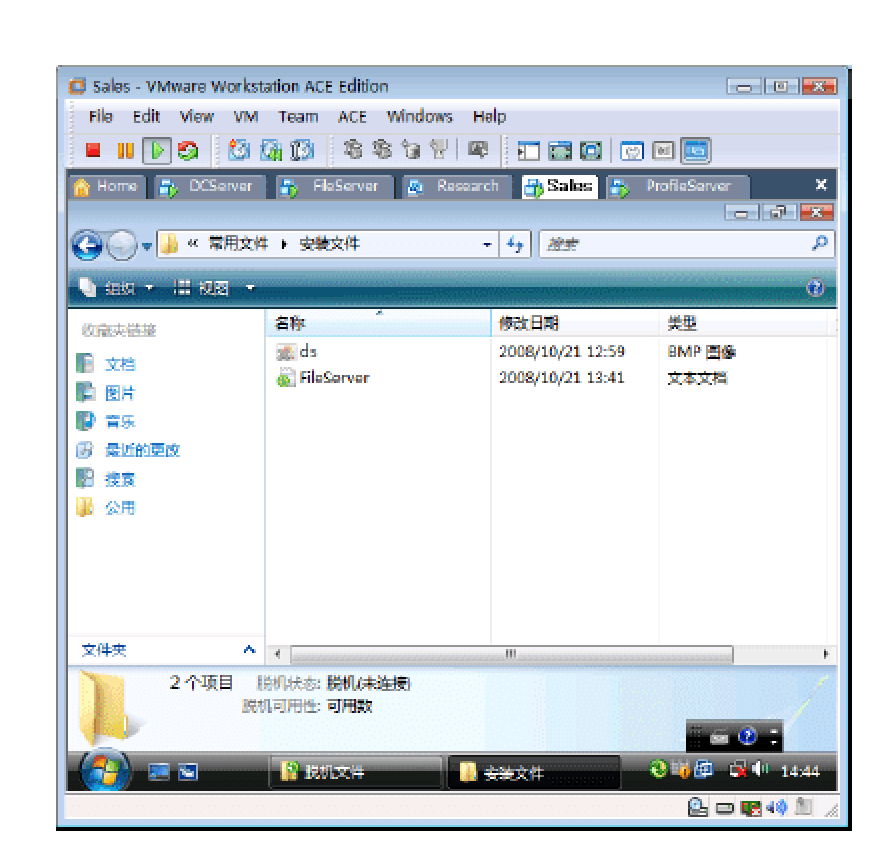


图 7-129　查看脱机的文件

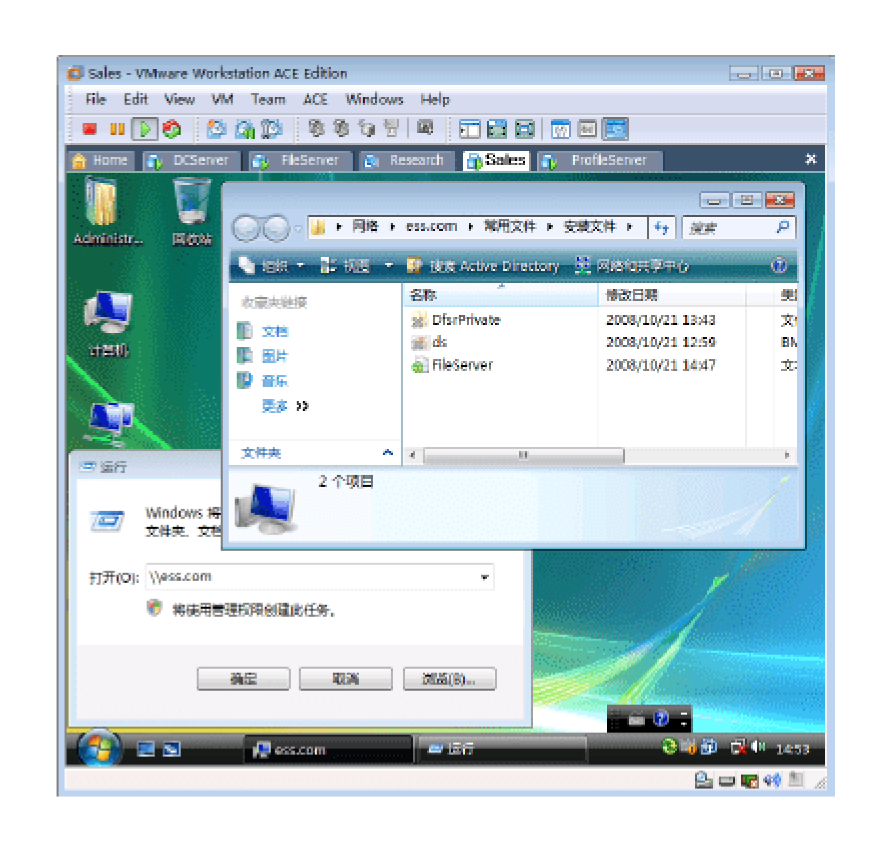


图 7-130　像联网时一样访问

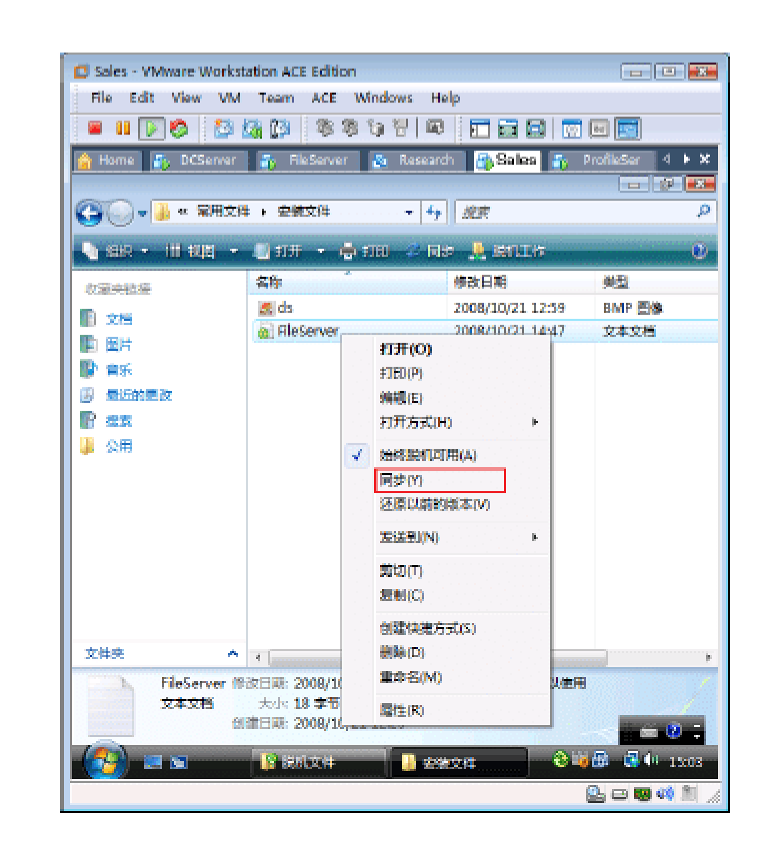


图 7-131　同步文件

7.6　限制文件夹的大小

在文件服务器文件夹的“配额管理”节点上，可以执行下列任务。

- 通过创建配额来限制卷或文件夹使用的空间，并在接近或达到配额限制时生成通知。
- 生成应用于卷或文件夹中所有现有子文件夹以及将来创建的任何子文件夹的自动应用配额。
- 定义可以很容易应用于新的卷或文件夹然后可以在整个组织中使用的配额模板。

例如，可以执行以下任务。

- 对用户的个人服务器文件夹设置 200 MB 的限制，并在超过 180 MB 存储空间时通知你和用户。
- 对组的共享文件夹设置灵活的 500 MB 配额。达到此存储限制时，将通过电子邮件通知组中的所有用户，存储配额已临时扩展到 520 MB，以便用户可以删除不必要的文件并符合预设的 500 MB 配额策略。
- 临时文件夹达到 2 GB 时接收通知，然而不对该文件夹的配额设置任何限制，因为这是服务器上运行的服务所需。

7.6.1　示例：创建文件夹限额

设置 FileServer 服务器上的“安装文件”文件夹的大小。限制为 200 MB。

① 选择“开始”→“程序”→“管理工具”→“文件服务器资源管理器”命令。

② 如图 7-132 所示，在“文件服务器资源管理器”对话框中，单击“创建配额”按钮。

③ 如图 7-133 所示，在出现的对话框中，指定使用配额的文件夹。选中“在路径上创建配额”单选按钮。选择“从此配额模板派生属性(推荐选项)”单选按钮，从下拉列表中选择“针对用户的 200 MB 限制报告”选项，单击“创建”按钮。

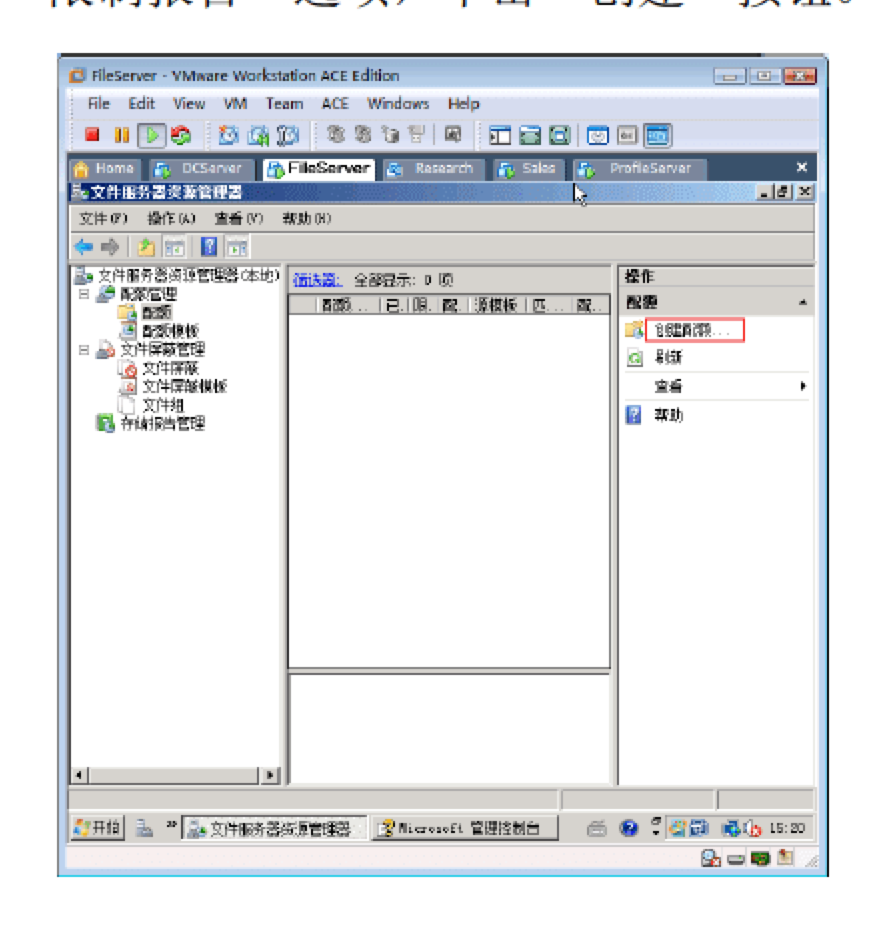




图 7-132　创建配额

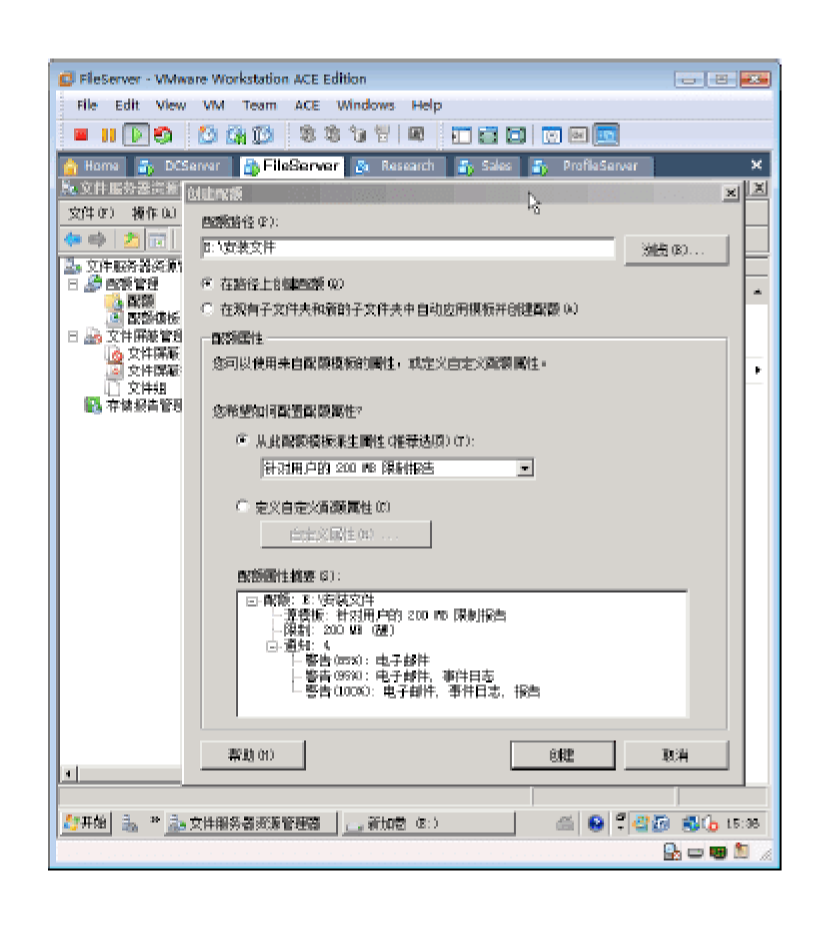


图 7-133　选定目录

④ 将一个 300 MB 的视频文件复制到“安装文件”，提示磁盘空间不足，如图 7-134 所示。

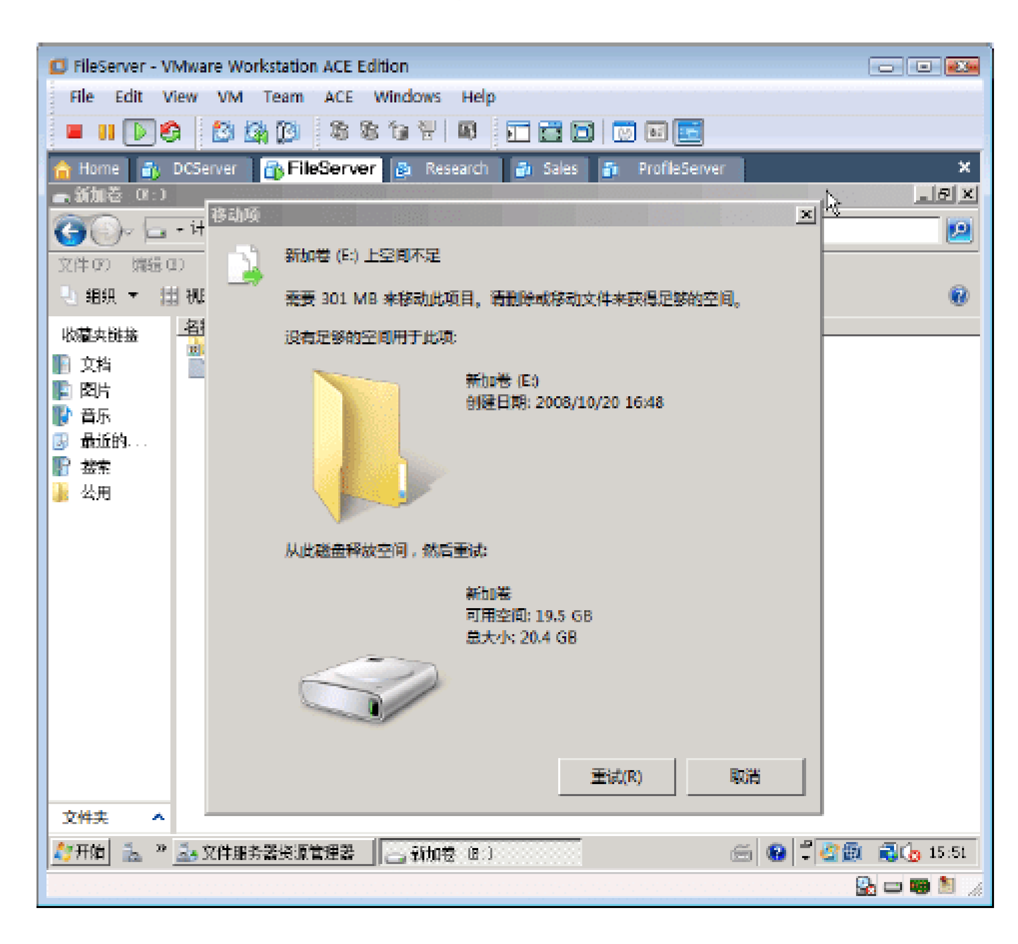


图 7-134　文件夹限额生效

7.6.2　管理配额模板

如图 7-135 所示，单击“配额模板”，可以创建配额模板。也可以双击现有的配额模板，编辑现有模板。

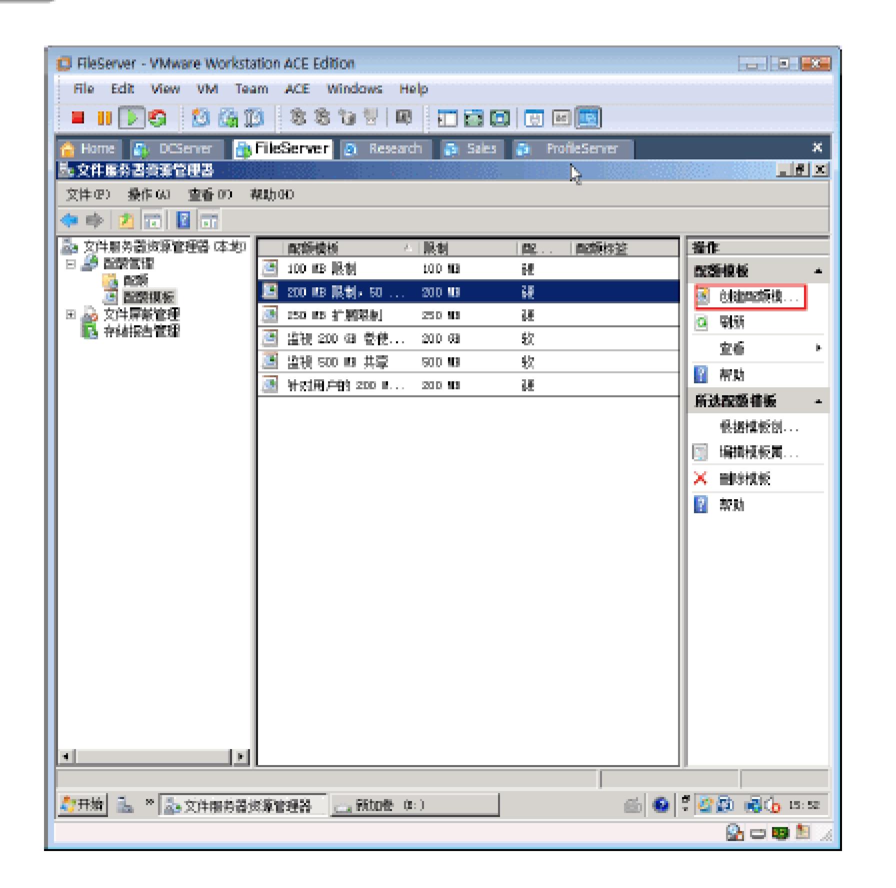


图 7-135　创建或编辑配额模板

7.7　限制文件夹存放的文件类型

我们可以指定某个文件夹能够存放的文件类型，它是基于文件的扩展名来控制的。通过创建文件屏蔽来控制用户可以保存的文件类型以及在用户尝试保存未经授权的文件时生成通知。定义可以应用于新的卷或文件夹以及可以在整个组织中使用的文件屏蔽模板。还创建增强文件屏蔽规则灵活性的文件屏蔽例外。

例如：确保服务器上的个人文件夹中未存储任何音乐文件，还可以允许存储支持法律权限管理或符合公司策略的特定媒体文件类型。在该情况下，可能需要为公司的副总授予在个人文件夹中存储任何文件类型的特殊权限。

执行屏蔽进程，在共享文件夹中存储可执行文件时通过电子邮件通知你，其中包含存储文件的用户和文件的准确位置等信息，以便采取相应的预防措施。

7.7.1　创建文件屏蔽

如图 7-136、图 7-137 所示，创建文件屏蔽，拒绝在“安装文件”文件夹以及子文件夹中存放图片文件。

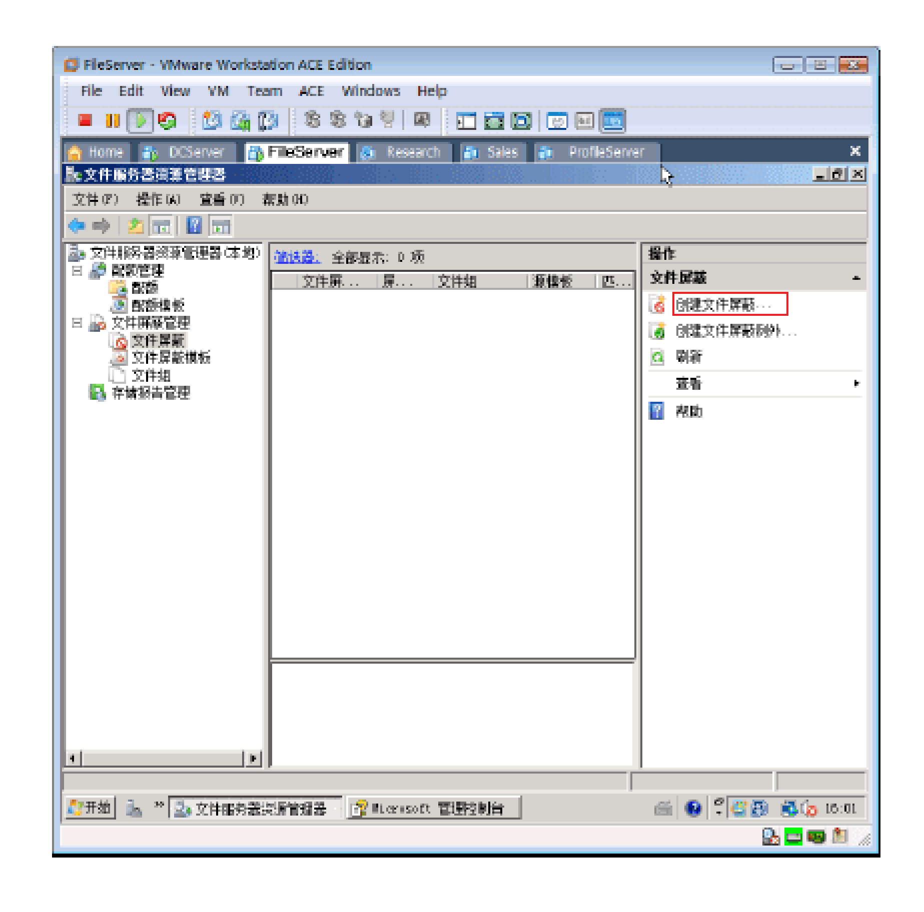


图 7-136　创建文件屏蔽

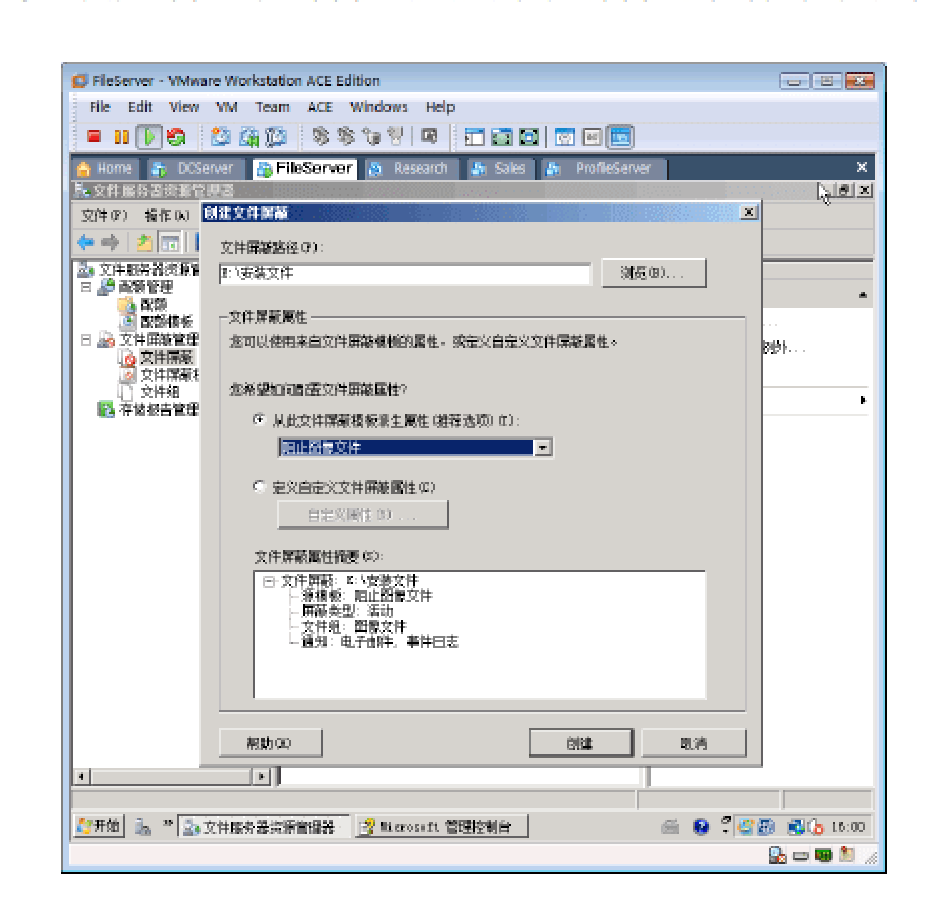


图 7-137　指定目录和屏蔽类型

如图 7-138 所示，在 E 盘根目录下创建一个图片 test.bmp，发现不能将该文件拖曳到 E:\安装文件目录下，提示用户没有权限。

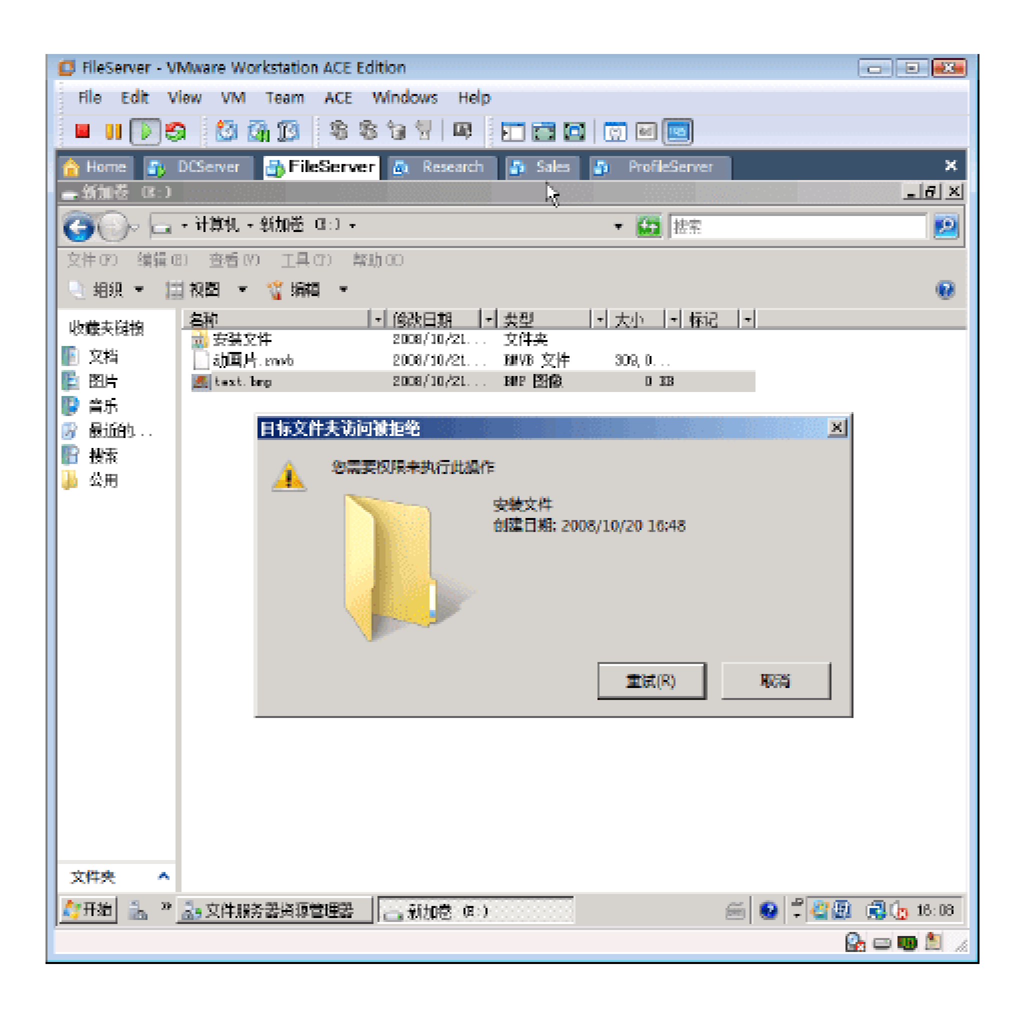


图 7-138　验证文件屏蔽

7.7.2　创建文件屏蔽例外

在“安装文件”文件夹中，有一个 Picture 子文件夹，要求能够存储图片，这时就需要创建一个文件屏蔽例外。

① 如图 7-139 所示，单击“创建文件屏蔽例外”按钮。

② 如图 7-140 所示，在出现的对话框中，输入“E:\安装文件\Picture”，选中“图像文件”复选框。单击“确定”按钮。

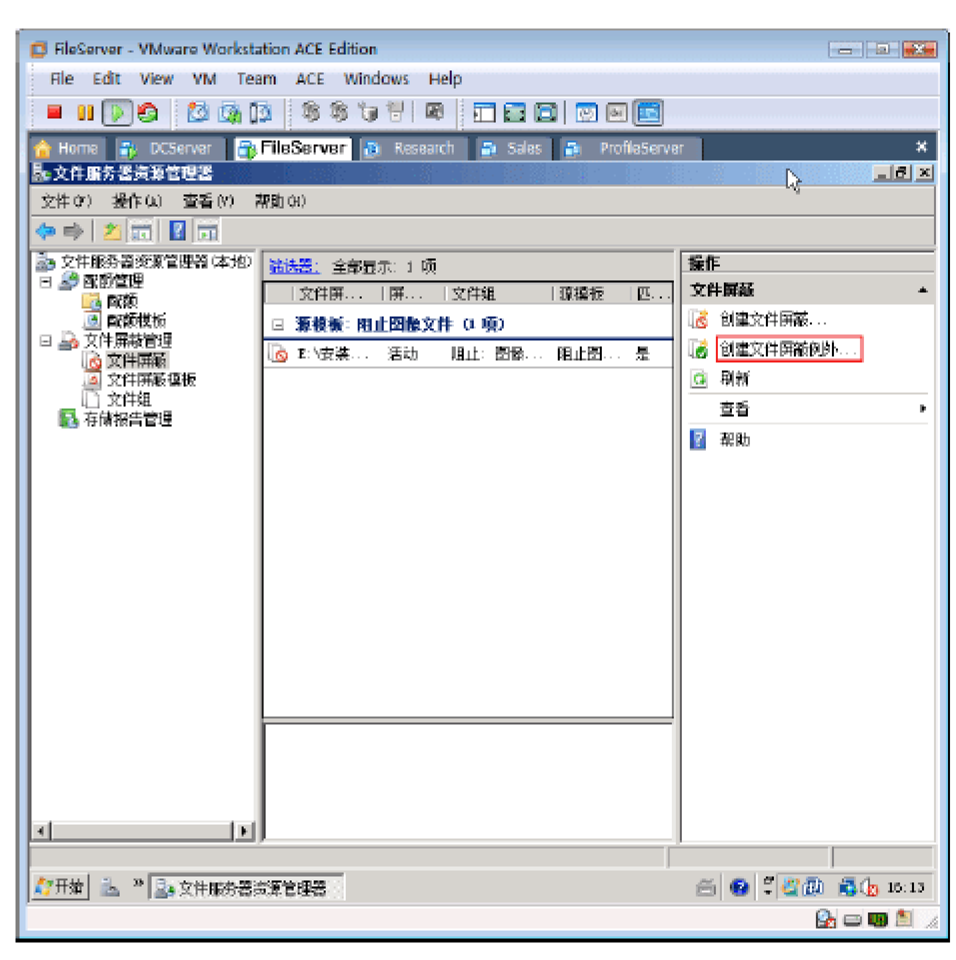
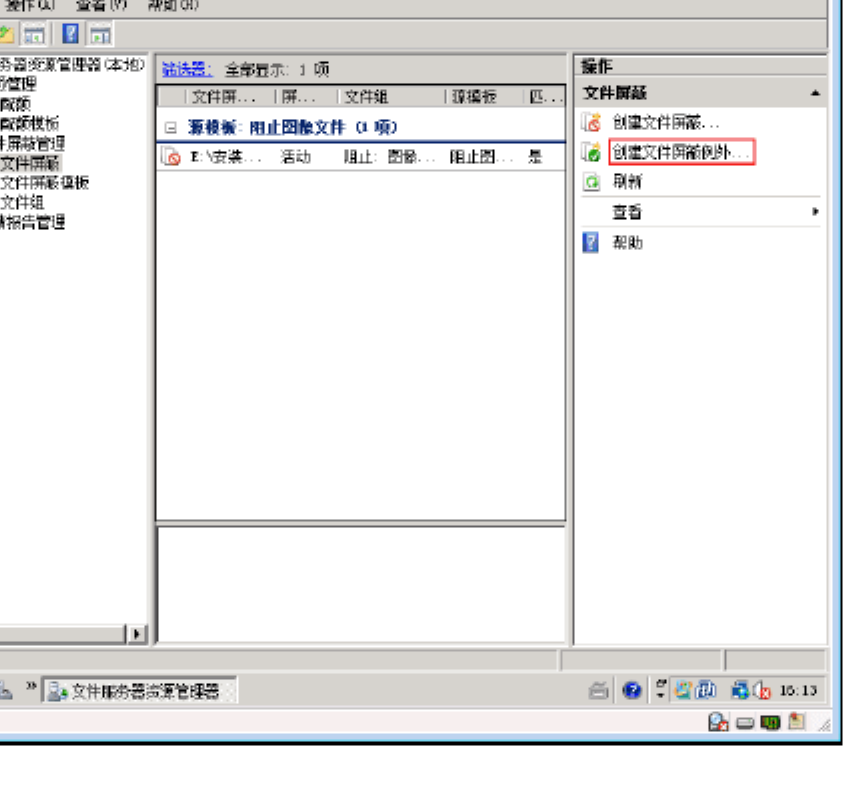



图 7-139　创建文件屏蔽例外

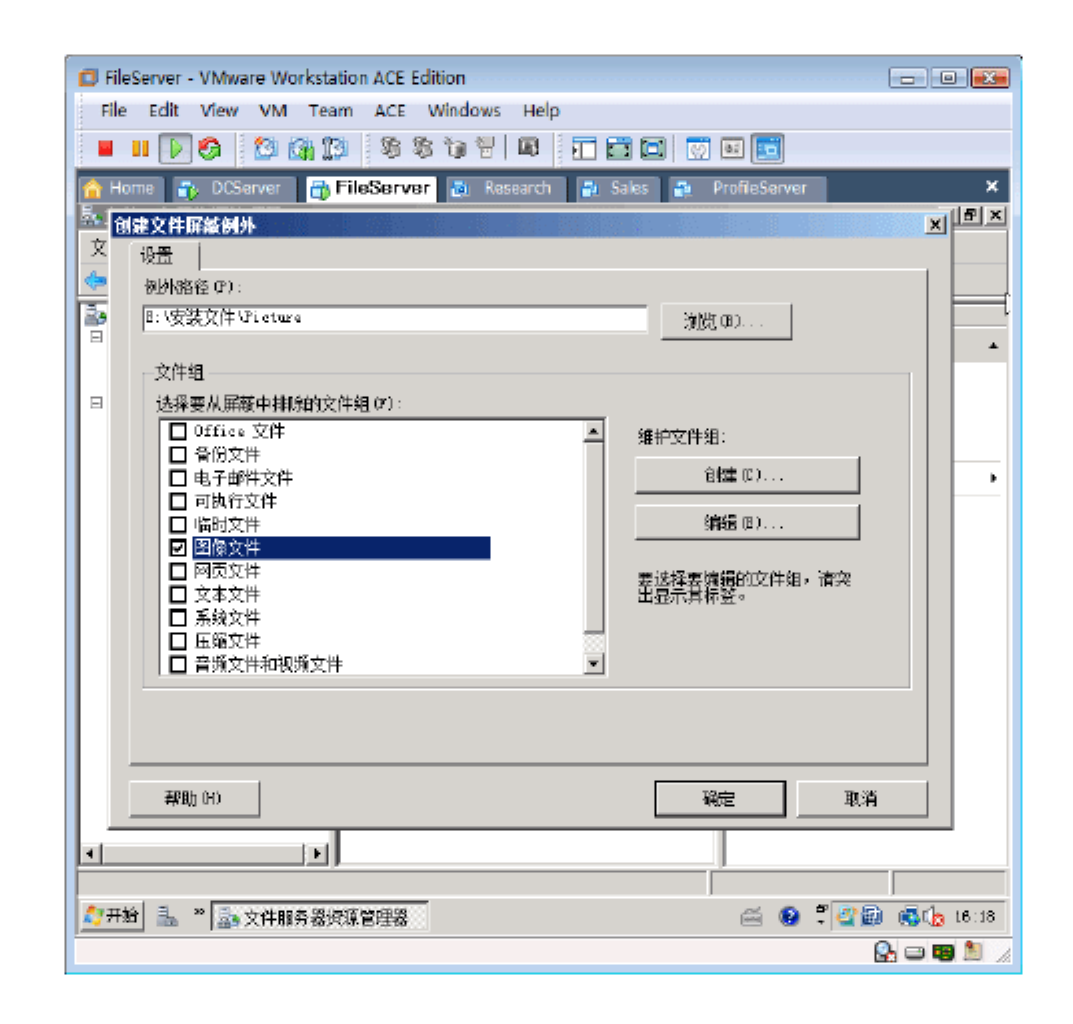


图 7-140　指定目录和例外的文件类型

③ 如图 7-141 所示，现在在“安装文件”夹的 Picture 目录下可以存放图片文件。

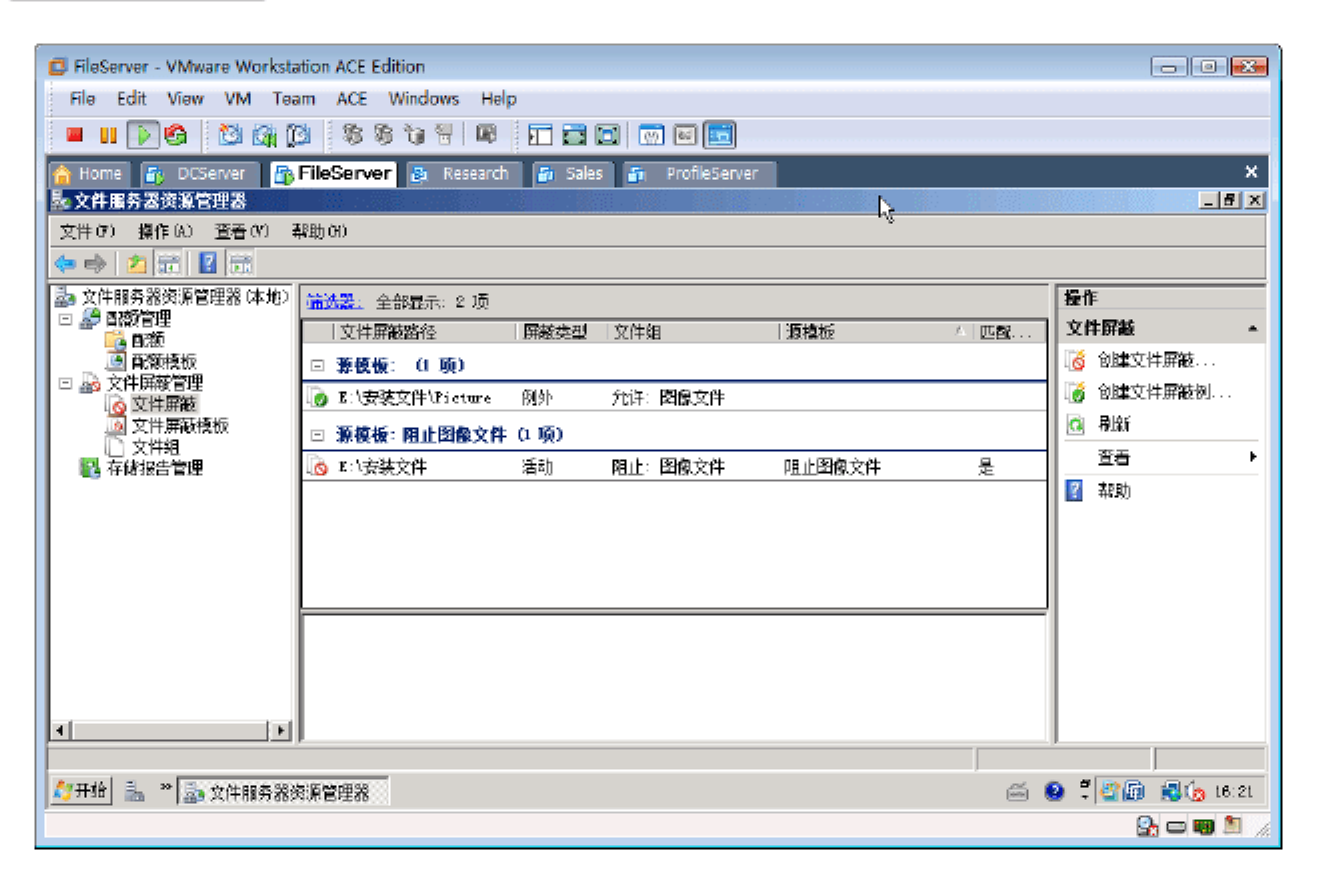


图 7-141　文件屏蔽例外

7.7.3　管理文件组

文件组可以编辑和创建，文件屏蔽就是基于文件的扩展名来控制的。

① 如图 7-142 所示，选择“文件组”，单击“创建文件组”按钮，可以创建新的文件组。

② 如图 7-143 所示，双击图片文件，可以修改图片文件包括的文件扩展名，也可以指定排除的文件名。

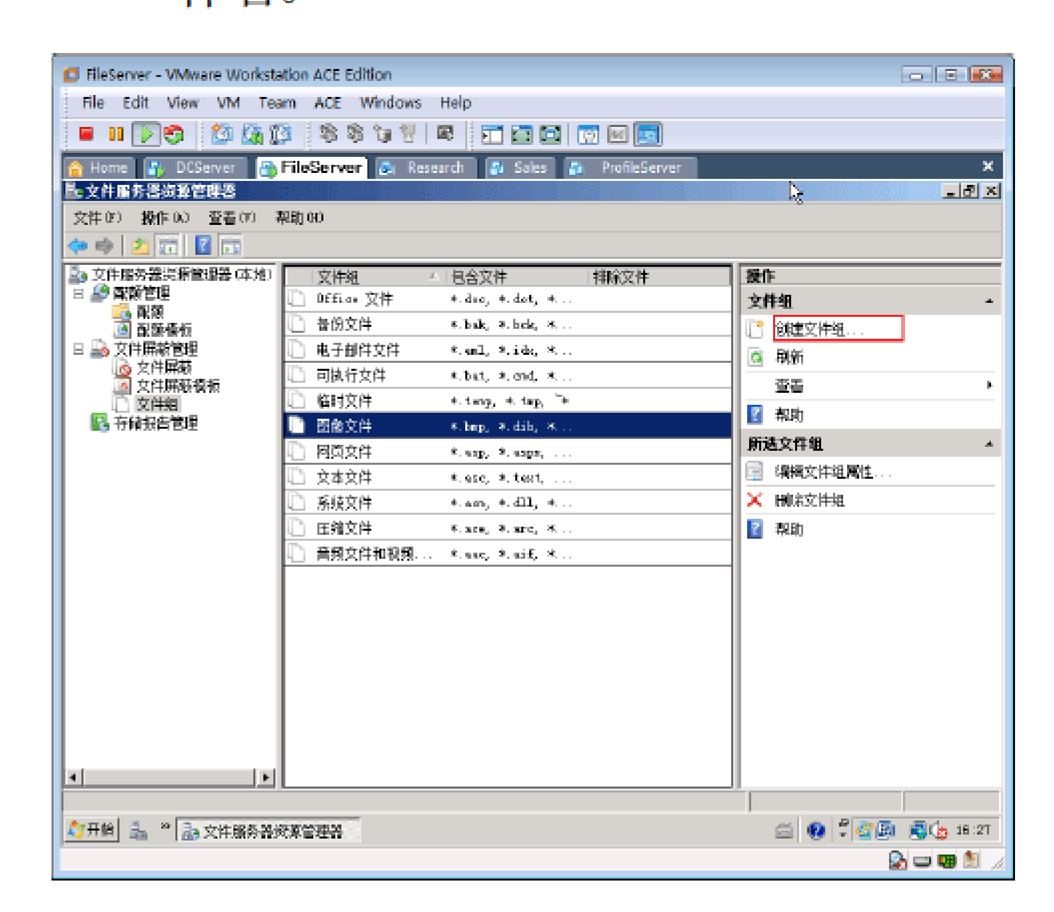


图 7-142　创建文件组

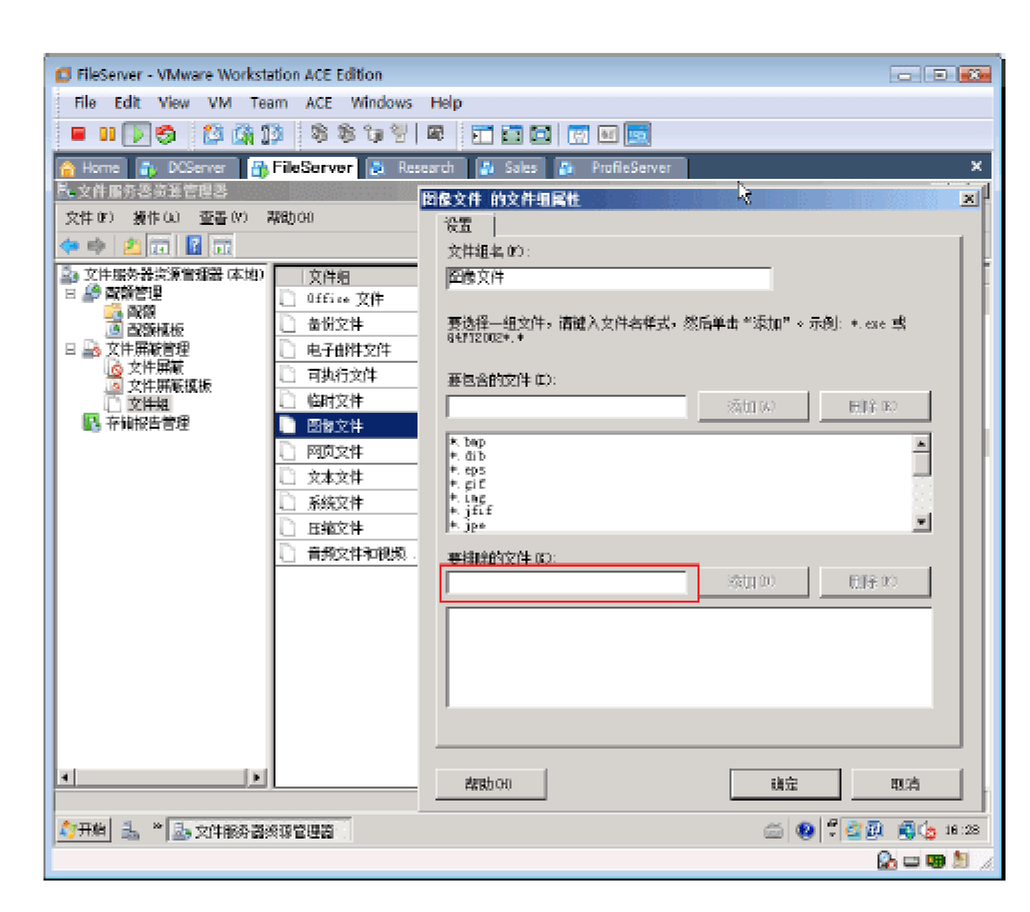


图 7-143　可以排除特定的文件名

第 8 章　监视和优化性能

通过查看 Windows 日志可以发现系统运行过程中出现的错误、警告以及信息，也能够看到安全审核记录的信息。通过查看日志中的错误，可以知道系统内部出现的问题，为我们排除操作系统的疑难错误提供解决问题的线索。

可以订阅其他服务器的日志，这样可以在一个服务器上集中查看网络中服务器的日志，有利于发现较为普遍的错误和警告。比如在众多的服务器上出现了登录失败的记录，你就能够断定近期有人试图猜密码登录系统。

利用任务管理器可以实时监控服务器内存和 CPU 的使用情况，能够结束不响应的程序或进程，可以发现消耗内存和 CPU 的进程。

利用系统监视器检测系统性能，可以监控操作系统任何指标，比如网络流量，磁盘的读写，内存的使用情况以及 CPU 的使用。使用系统内置的数据收集器可以跟踪服务器运行，给出诊断报告，找到服务器的瓶颈。比如内存小，或磁盘读写慢，或 CPU 太慢等。

如果服务器安装了多个应用程序，或多个用户使用，通过使用 Windows 系统资源管理器，可以控制内存和 CPU 的分配。

关键词

- 管理 Windows 日志
- 订阅远程计算机的日志
- 利用任务管理器监控系统资源
- 利用“系统监视器”检测系统性能
- 监控远程计算机性能
- 跟踪检测计算机性能
- 使用 Windows 系统资源管理器

8.1 Windows 日志

Windows 日志类别包括以下在早期版本的 Windows 中可用的日志：应用程序、安全和系统日志。此外还包括两个新的日志：安装程序日志和 Forwarded Events 日志。Windows 日志用于存储来自旧版应用程序的事件以及适用于整个系统的事件。

8.1.1 事件日志的类型

如图 8-1 所示，打开事件查看器，可以看到以下日志类型。

1. 应用程序日志

应用程序日志包含由应用程序或程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。程序开发人员决定记录哪些事件。

2. 安全日志

安全日志包含诸如有效和无效的登录尝试等事件，以及与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理员可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，则对系统的登录尝试将记录在安全日志中。

3. 安装程序日志

安装程序日志包含与应用程序安装有关的事件。

4. 系统日志

系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。系统组件所记录的事件类型由 Windows 预先确定。

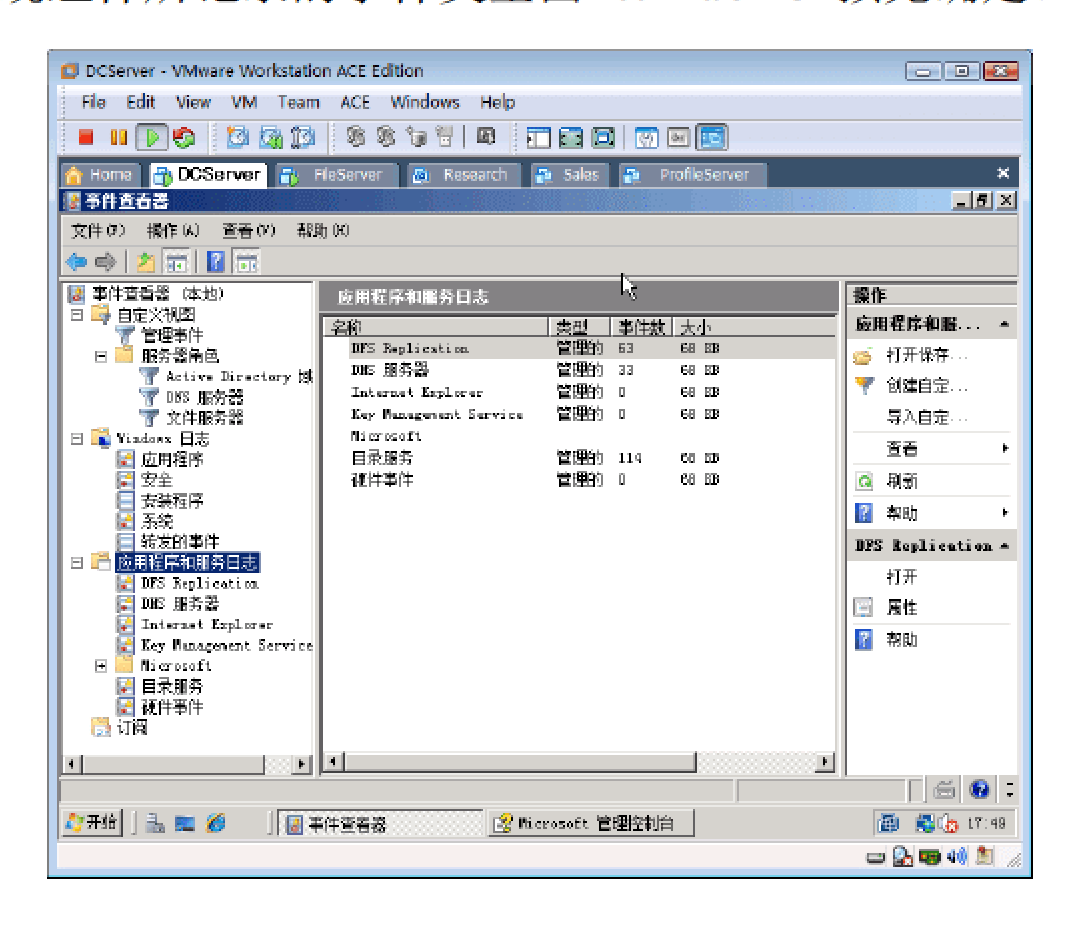


图 8-1 日志类型

5. Forwarded Events 日志

Forwarded Events 日志用于存储从远程计算机收集到的事件。若要从远程计算机收集事件，必须创建

事件订阅。

6. 应用程序和服务日志

应用程序和服务日志是一种新类别的事件日志。这些日志存储来自单个应用程序或组件的事件，而非可能影响整个系统的事件。

此类别的日志包括四个子类型：管理日志、操作日志、分析日志和调试日志。管理日志中的事件尤其受使用事件查看器解决问题的 IT 专业人士的关注。管理日志中的事件应该提供有关如何对事件做出响应的指南。操作日志中的事件对 IT 专业人士也很有用，但他们可能需要更多解释。

管理日志和调试日志不那么友好。分析日志存储跟踪问题事件，通常需要大量记录。调试日志由开发人员在调试应用程序时使用。默认情况下，分析日志和调试日志都为隐藏和禁用状态。若要使这些日志可见，请按照显示或隐藏分析日志和调试日志中的步骤操作。若要启用这些日志，请按照启用分析日志和调试日志中的步骤操作。

8.1.2 事件属性

- 来源：记录事件的软件，可以是程序名(如 SQL Server)，也可以是系统或大型程序的组件(如驱动程序名)。例如，Elnkii 表示 EtherLink II 驱动程序。
- 事件 ID：标识特定事件类型的编号。描述的第一行通常包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID。此类事件的描述的第一行是“事件日志服务已启动”。产品支持代表可以使用事件 ID 和来源来解决系统问题。
- 级别：事件严重性的分类。以下事件严重性级别可能出现在系统和应用程序日志中。
  - 信息。指明应用程序或组件发生了更改，如操作成功完成、已创建了资源，或已启动了服务。
  - 警告。指明出现的问题可能会影响服务器或导致更严重的问题(如果未采取措施)。
  - 错误。指明出现了问题，这可能会影响触发事件的应用程序或组件外部的功能。
  - 关键。指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复。

  以下事件严重性级别可能出现在安全日志中，如图 8-2 所示。

  - Success Audit。指明用户操作成功。
  - 审核失败。指明用户操作失败。
  - 在事件查看器的正常列表视图中，这些分类都由符号表示。
- 用户：事件发生所代表的用户的名称。如果事件实际上是由服务器进程所引起的，则此名称为客户端 ID；如果没有发生模仿的情况，则为主 ID。如果适用，安全日志项同时包含主 ID 和模仿 ID。当服务器允许一个进程采用另一个进程的安全属性时就会发生模拟的情况。
- 操作代码：包含标识活动或应用程序引起事件时正在执行的活动中的点的数字值。例如，初始化或关闭。
- 日志：已记录事件的日志的名称。
- 任务类别：用于表示事件发行者的子组件或活动。
- 关键字：可用于筛选或搜索事件的一组类别或标记。示例包括“网络”、“安全”或“未找到资源”。
- 计算机：发生事件的计算机的名称。该计算机名称通常为本地计算机的名称，但它可能是已转发事件的计算机的名称，或者可能是名称更改之前的本地计算机的名称。

■ 日期和时间：记录事件的日期和时间。

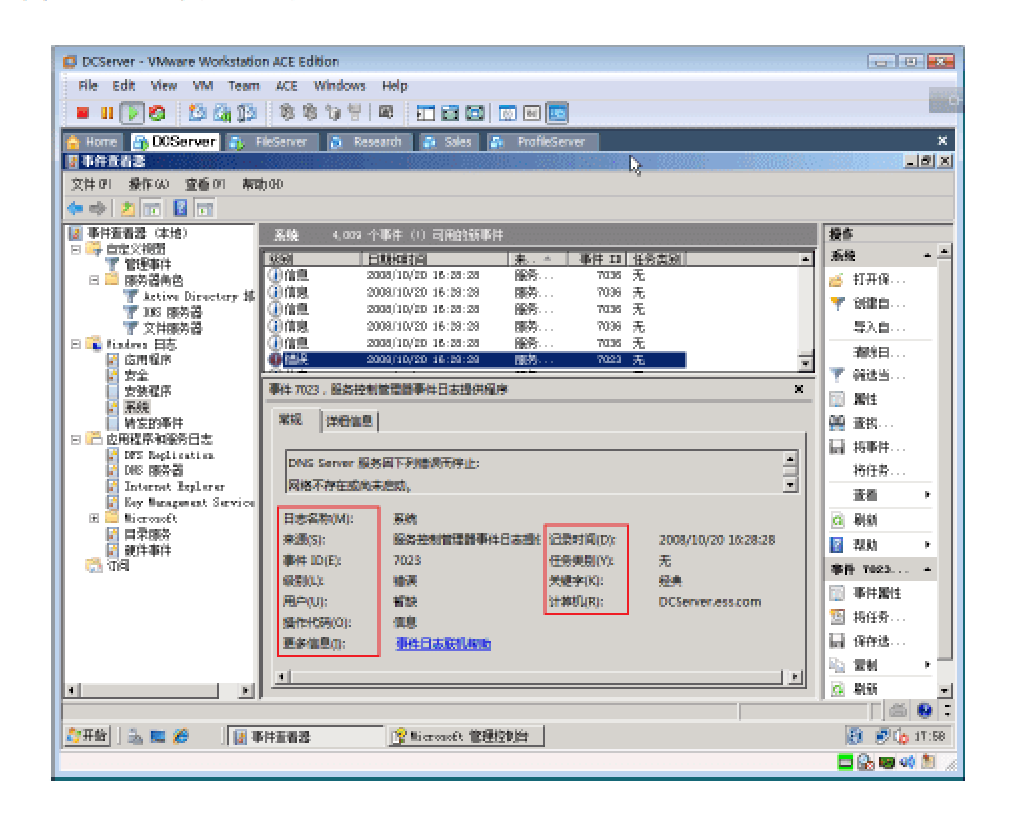


图 8-2 日志属性

8.1.3 自定义视图

在早期版本的事件查看器中，可以筛选事件日志中的事件。为创建筛选器，指定了一组用于确定日志中哪些事件可见和哪些事件隐藏的规则。例如，可以指定只有等级值为“错误”或“警告”的事件才应该可见。

筛选事件的功能非常关键。只需要重点关注适用于正在调查的问题的那些事件。事件查看器的最新版本将筛选的概念扩展到超出单个事件日志以外。它使你可以创建一组规则，这些规则选择来自所指定源的事件，并只显示来自其属性值满足这些规则的那些源的事件。

创建只显示对于特定问题所关注的事件可能会需要很长时间。自定义视图提供了一种保存此工作的方式。创建只显示所关注记录的筛选器后，就可以提供筛选器的名称并将其保存以供以后使用。这个保存的筛选器就是一个自定义视图。

示例：显示最近 7 天，系统出现的错误和警告。

① 如图 8-3 所示，单击“自定义视图”，单击“创建自定义视图”按钮。在打开的“创建自定义视图”对话框中，记录时间选择“最后 7 天”，事件类型选中“错误”和“警告”，按日志选中“系统”。单击“确定”按钮。

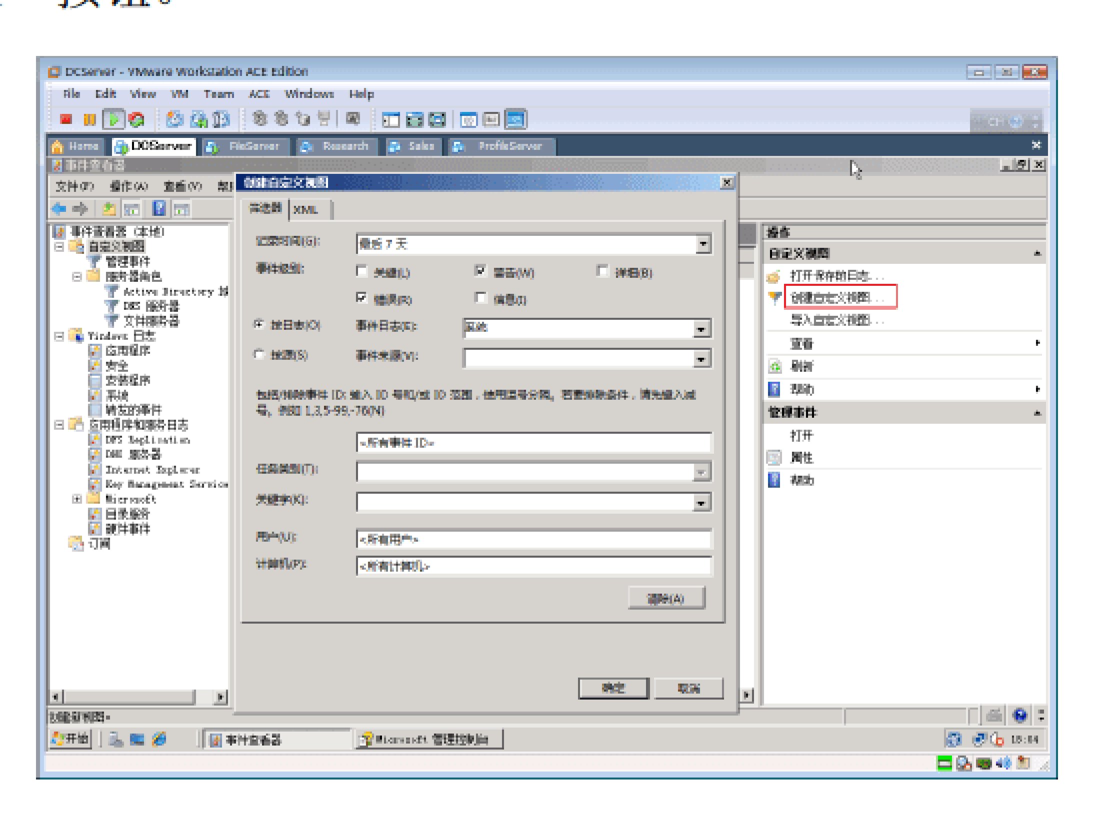


图 8-3 创建自定义视图

② 如图 8-4 所示，输入名称“最近 7 天的错误和警告”，单击“新建文件夹”按钮，输入“我的视图”。

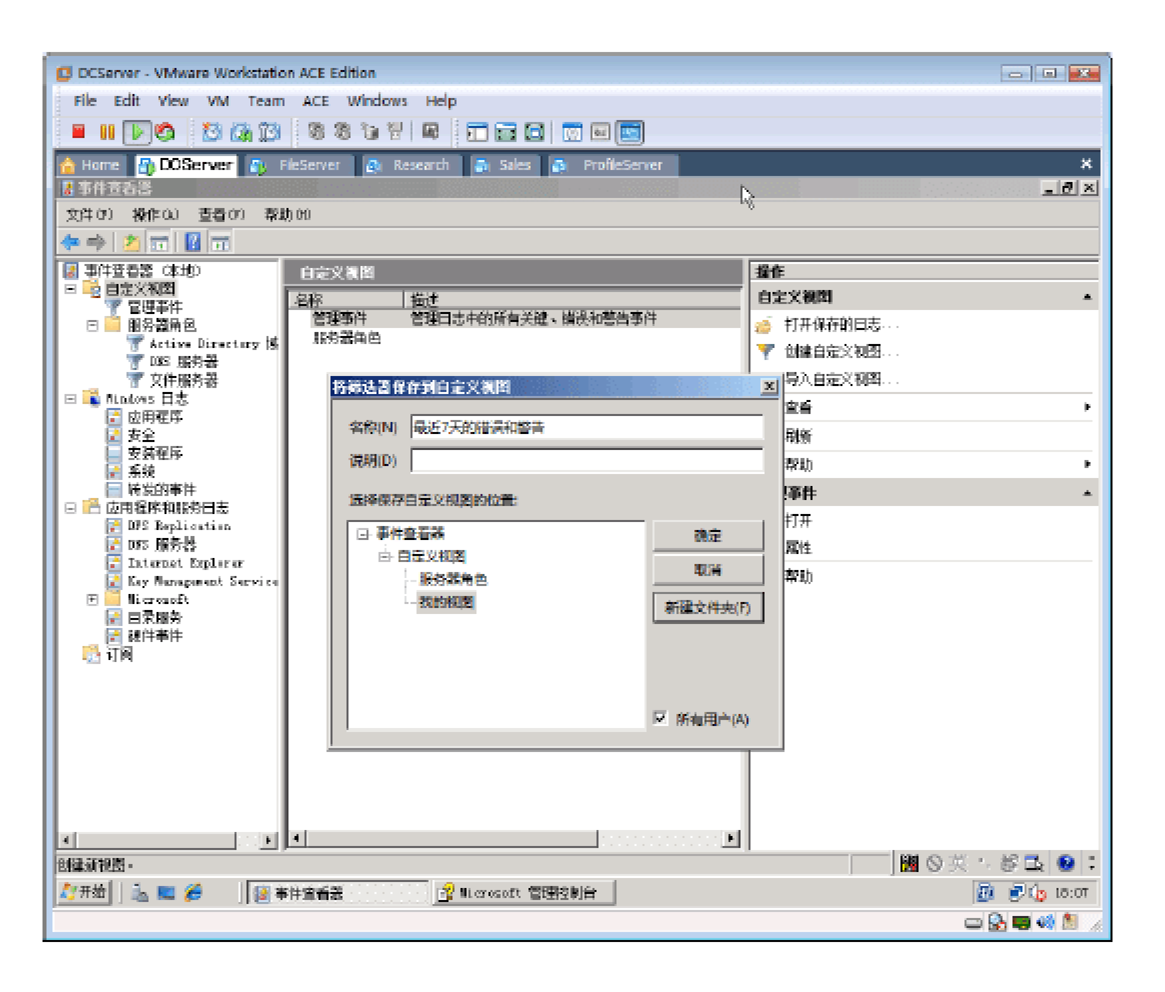


图 8-4　输入名称

③ 如图 8-5 所示，单击“我的视图”下的“最近 7 天的错误和警告”选项，可以看到筛选出来的系统产生的错误和警告。

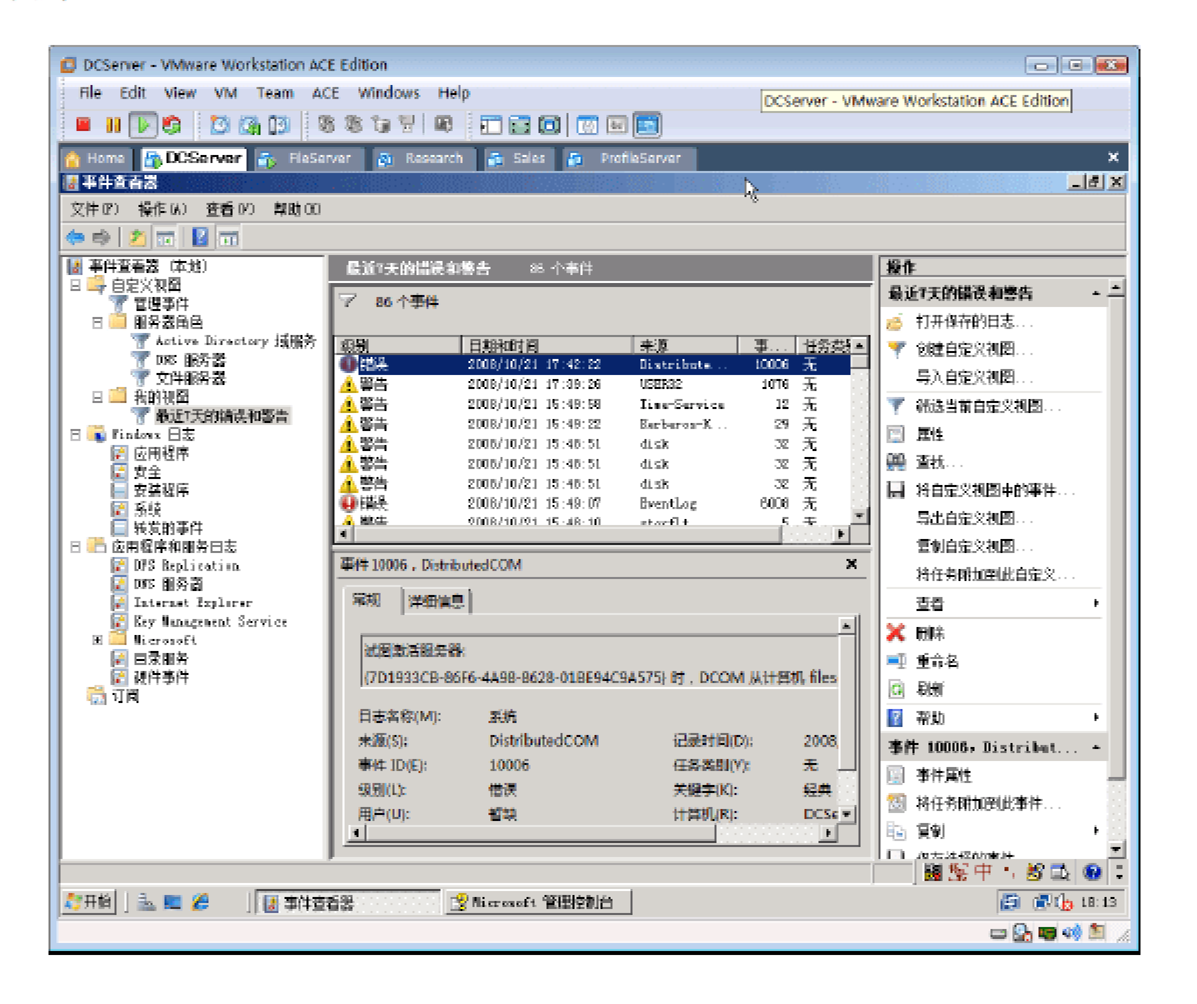


图 8-5　通过视图查看

8.1.4　管理日志

事件日志存储在文件中。这些文件的大小都有可以更改的默认最大值。可以通过使用 Windows 界面或命令行执行此过程。

① 如图 8-6 所示，展开“Windows 日志”→“系统”节点，单击“属性”按钮，在出现的“日志属性”对话框中，可以设置日志的存储位置，日志最大大小，清除日志，以及达到最大值后，设置日志保留策略。

- 按需要改写事件：日志文件已满时继续存储新事件。每个新传入事件替换日志中最旧的事件。
- 日志满时将其存档，不改写事件：必要时自动将日志存档。不改写任何事件。
- 不改写事件(手动清除日志)：手动而非自动清除日志。

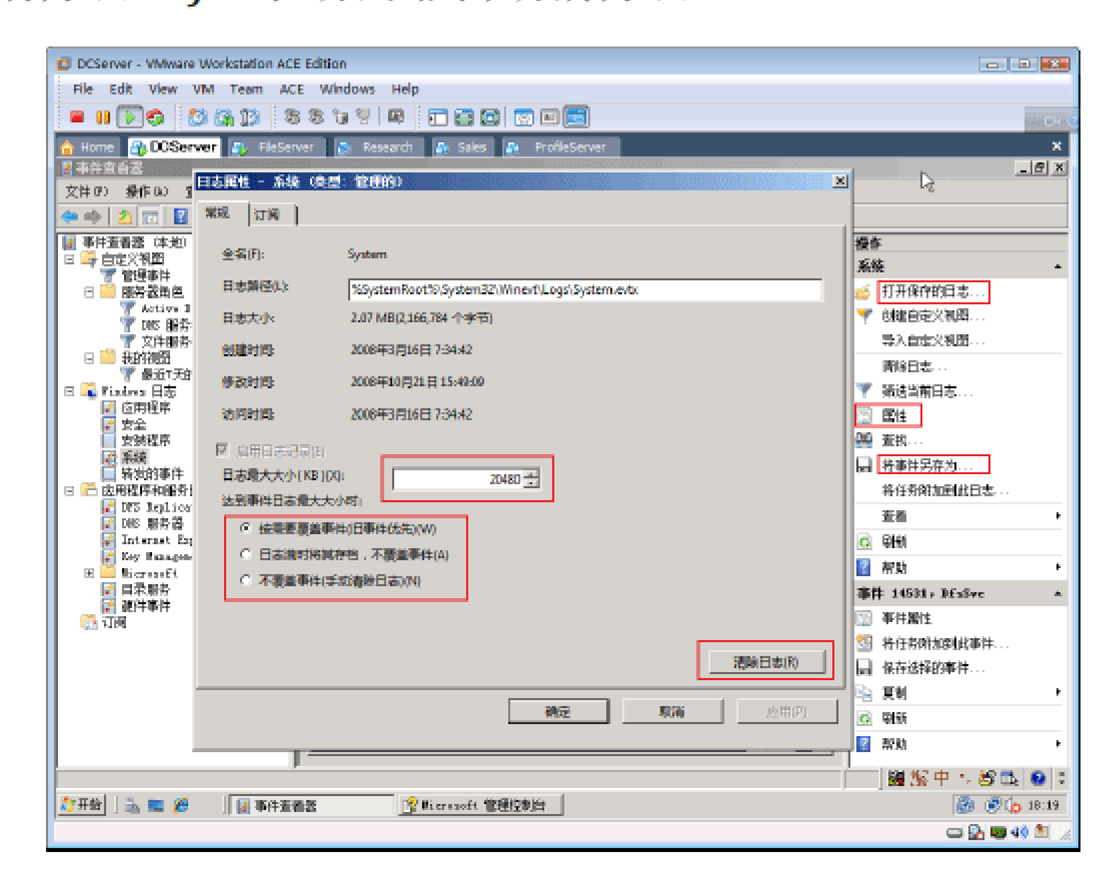


图 8-6　指定日志文件的大小和处理方式

② 单击“将事件另存为”选项，保存类型选择“事件属性”，输入文件名称“2008 年 10 月 21 日以前的系统日志”，单击“保存”按钮。

③ 如图 8-6 所示，单击“打开保存的日志”，浏览到“2008 年 10 月 21 日以前的系统日志”，单击“打开”按钮。

④ 如图 8-7 所示，可以看到保存的日志。

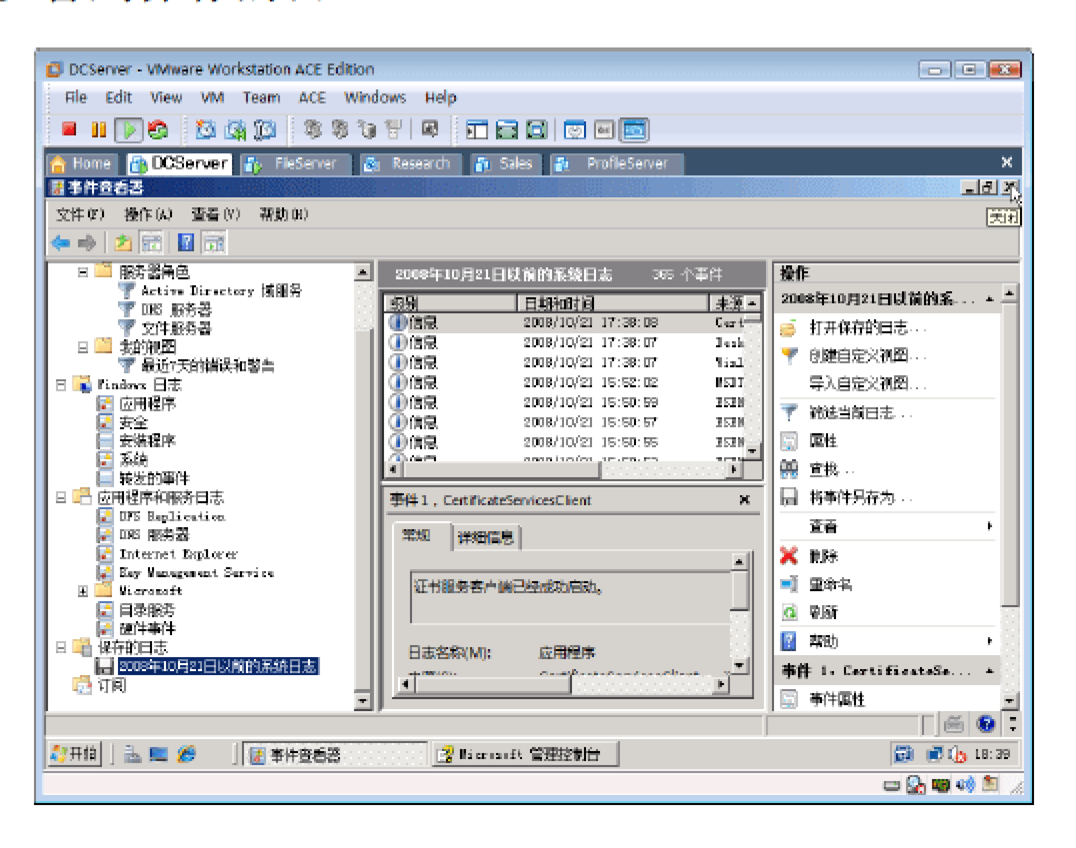


图 8-7　打开保存的日志

8.1.5　配置计算机以转发和收集事件

Windows 远程管理 (WinRM)是一个远程管理技术，它使得可以通过 HTTP 网络连接发送 WMI 命令。通过使用 WinRM 进行远程服务器管理，可以减少 DCOM 或者 RPC 的连接，只需要使用 HTTP 或者 HTTPS 就可以了，这对于跨越防火墙管理的场景非常有用(否则需要打开类似 TCP 135 这样的端口)。决定 Windows Server 2008 基于 WinRM 的事件订阅和 WinRS(Windows Remote Shell)来保证远程服务器运行正常以及在出现问题时在第一时间进行修复。

示例：订阅日志。

必须配置收集计算机(收集器)和每台将从其收集事件的计算机(源)，然后才能创建订阅来收集计算机上的事件。

配置 DCServer 服务器订阅 FileServer 服务器和 Server Core 计算机 ProfileServer 上的日志。

① 以域管理员账户登录到 FileServer，在命令提示符下输入 WinRM QuickConfig，然后按 Enter 键。

② 在“进行这些更改吗”提示符下，输入 Y。

③ 以域管理员的账户登录 ProfileServer。

④ 如图 8-8 所示，在命令提示符下输入 WinRM QuickConfig，然后按 Enter 键。

⑤ 如图 8-9 所示，在 “进行这些更改吗”提示符下，输入 Y。

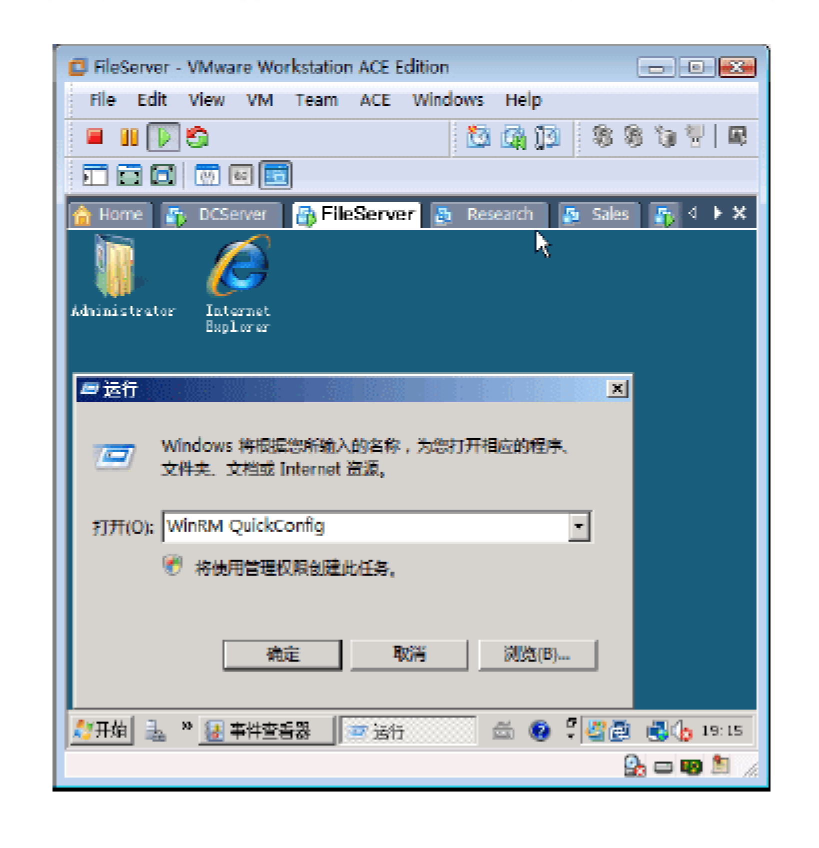


图 8-8　启用远程管理功能

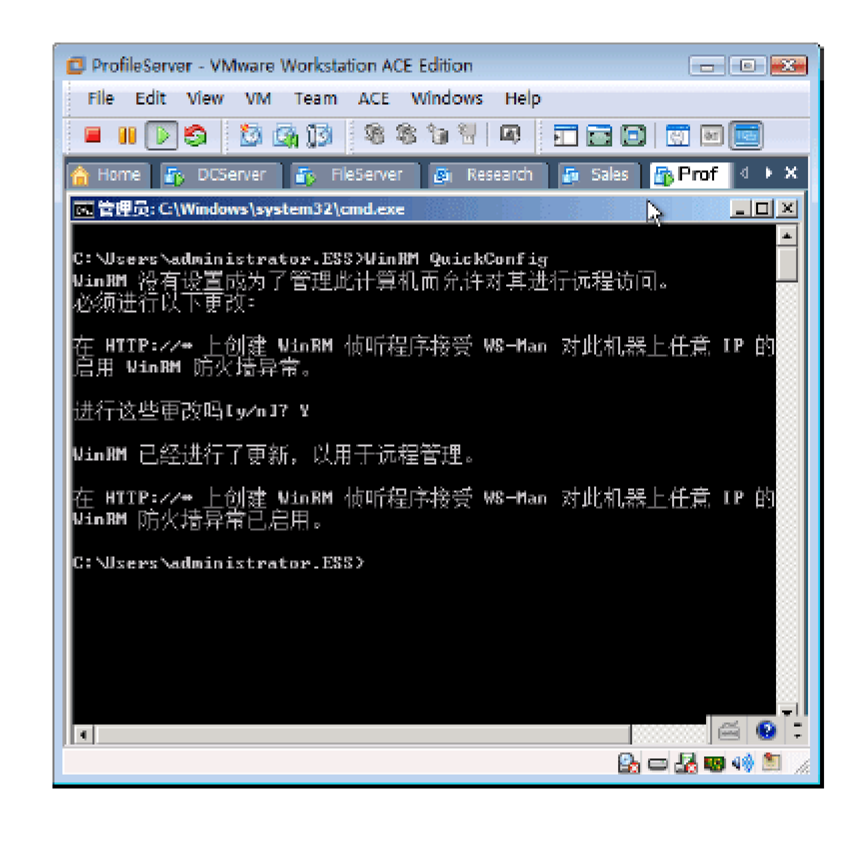


图 8-9　确认

⑥ 以域管理员的账户登录 DCServer。

⑦ 选择“开始”→“运行”命令，输入 MMC，单击“确定”按钮。

⑧ 在打开的 MMC 对话框中，选择“文件”→“添加/删除管理单元”命令，如图 8-10 所示。

⑨ 如图 8-11 所示，在“添加/删除管理单元”对话框中，选择“本地用户和组”选项，单击“添加”按钮，在出现的“选择目标机器”对话框中，选中“另一台计算机”单选按钮，输入 ProfileServer，单击“完成”按钮。

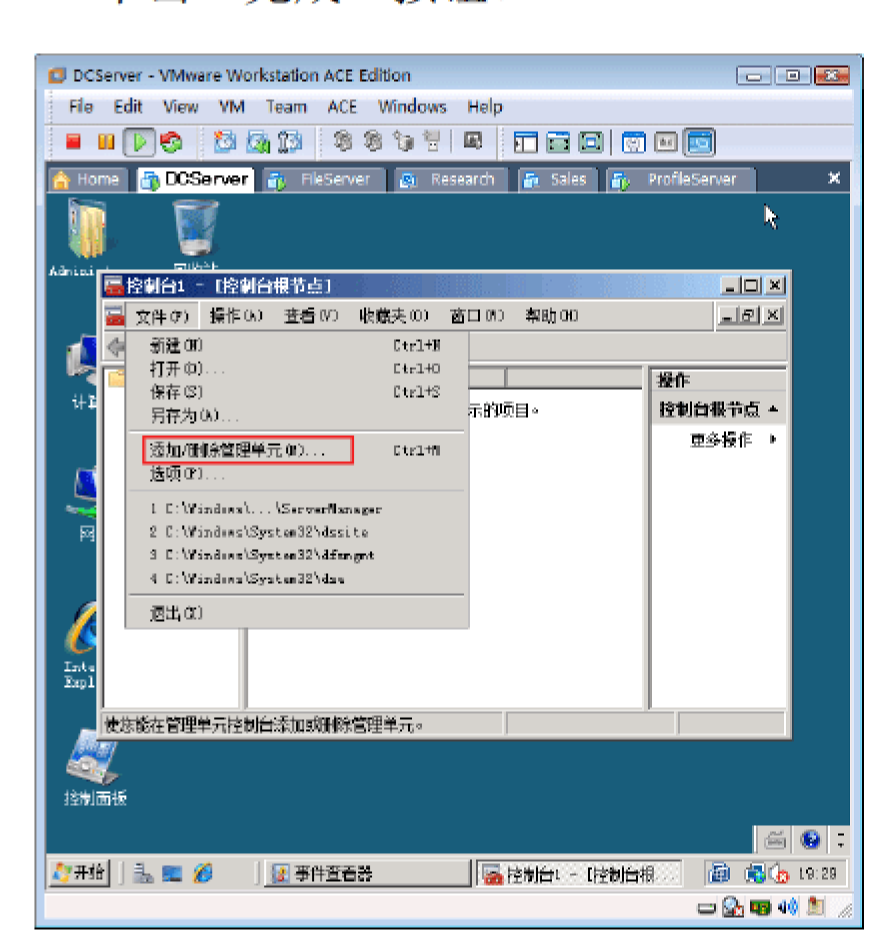


图 8-10　打开微软管理控制台

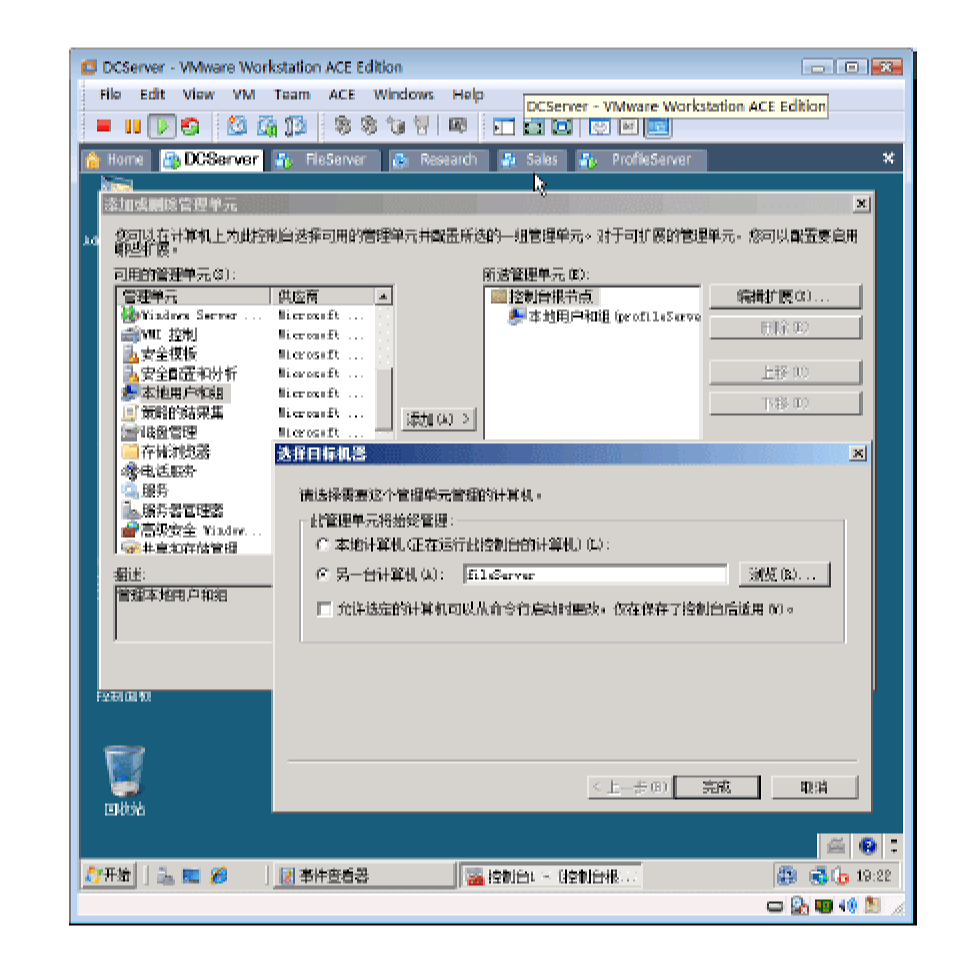


图 8-11　连接 Windows Server Core

⑩ 再次单击“添加”按钮，选择“另一台计算机”单选按钮，输入 fileServer，单击“完成”按钮。

⑪ 单击 ProfileServer 计算机的本地用户和组，双击 Event log readers 组，在出现的 Event Log readers 属性对话框中，单击“添加”按钮。

⑫ 在“选择用户、计算机或组”对话框中，单击“对象类型”按钮，如图 8-12 所示。

⑬ 如图 8-13 所示，在出现的“对象类型”对话框中，选中“计算机”复选框，单击“确定”按钮。

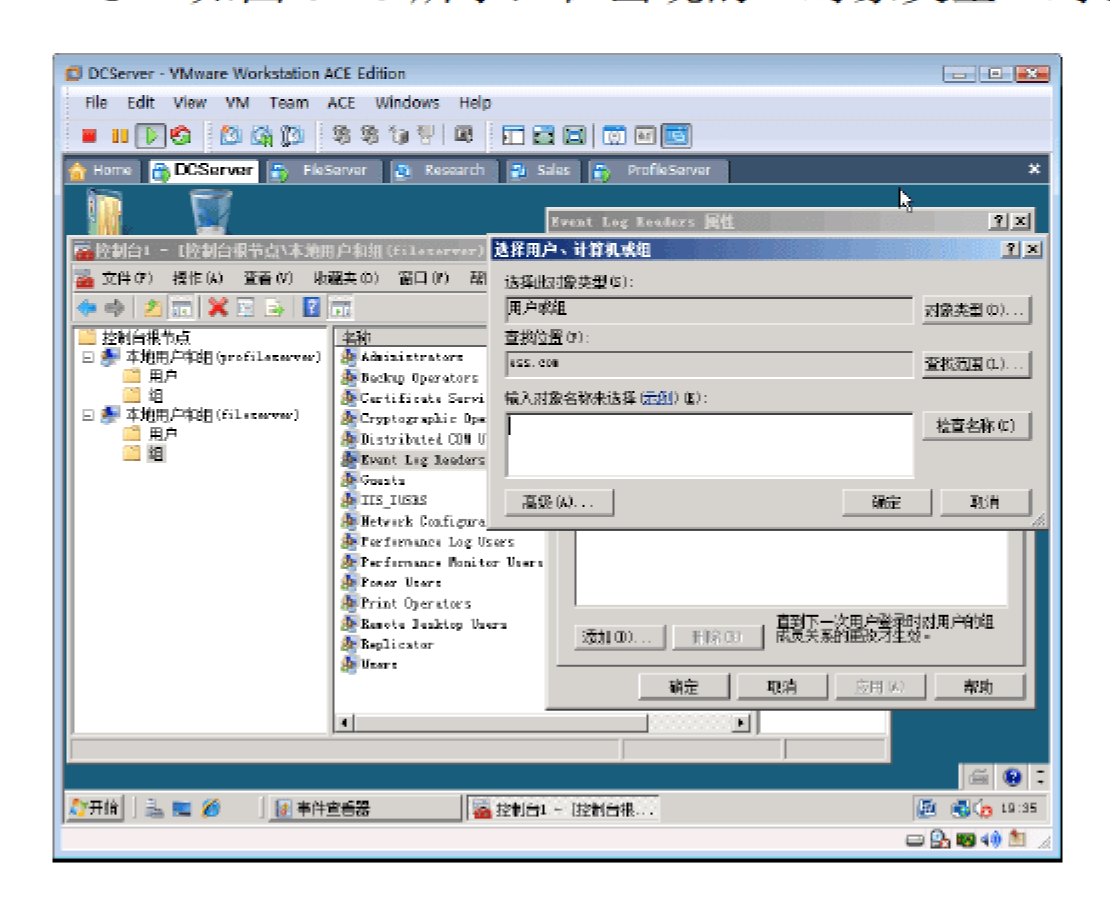


图 8-12　更改对象类型

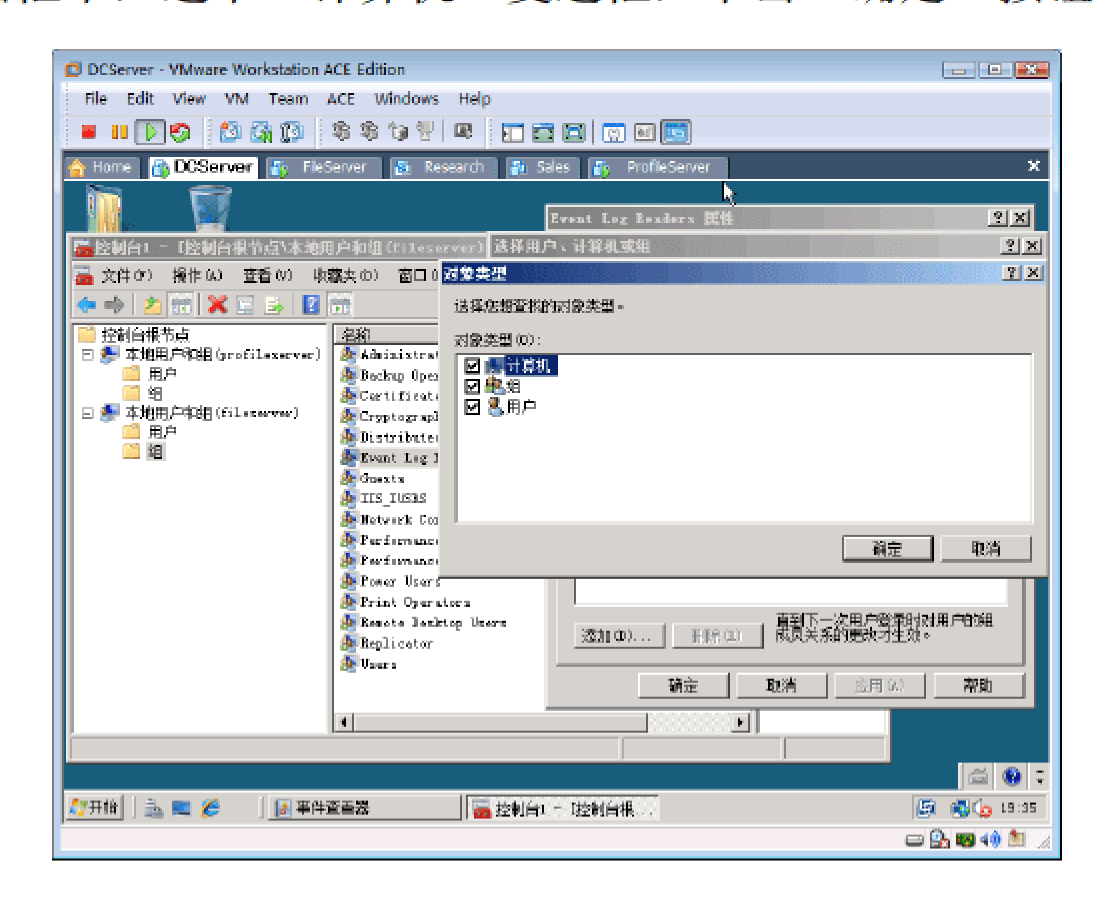


图 8-13　选中计算机

⑭ 如图 8-14 所示，输入 DCSERVER，单击“确定”按钮。

⑮ 以同样的方式，将计算机账户 DCSERVER 添加到 FileServer 的 Event log readers 组。这样 DCServer 计算机就能够订阅 FileServer 和 ProfileServer 的日志。

⑯ 以管理员的账户登录 DCSERVER。打开“事件查看器”。

⑰ 如图 8-15 所示，单击“订阅”选项，单击“创建订阅”选项，输入订阅名称“查询 FileServer 和 ProfileServer 上的系统错误事件”，目标日志选择“转发的事件”。

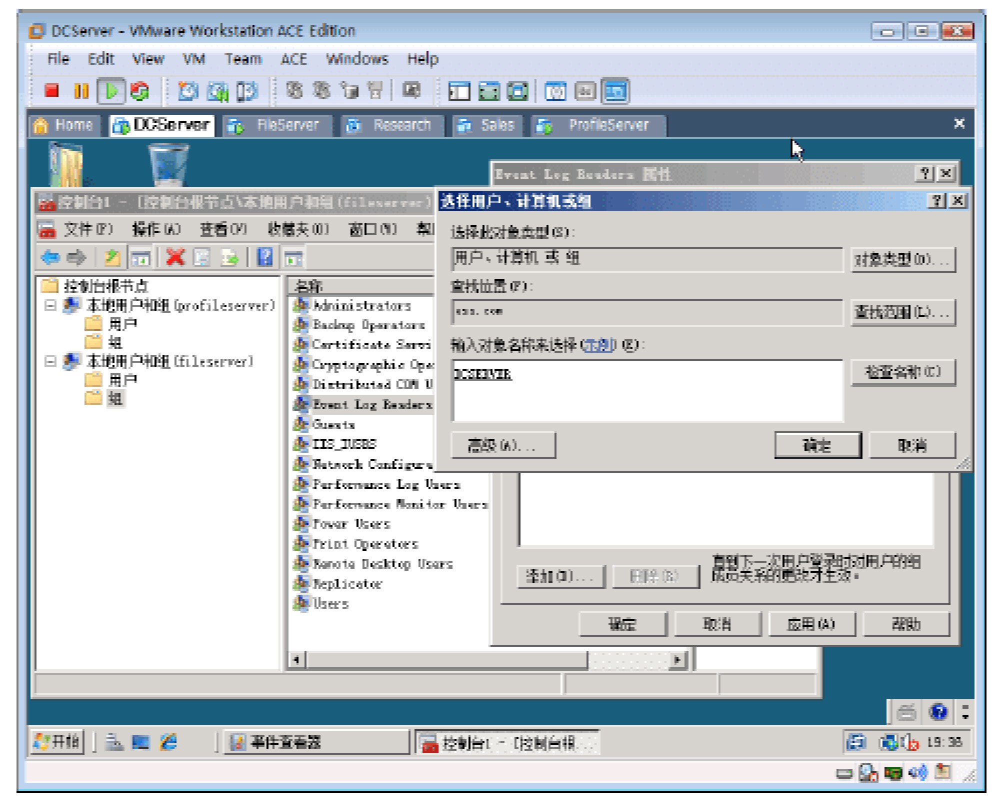


图 8-14　输入 DCSERVER

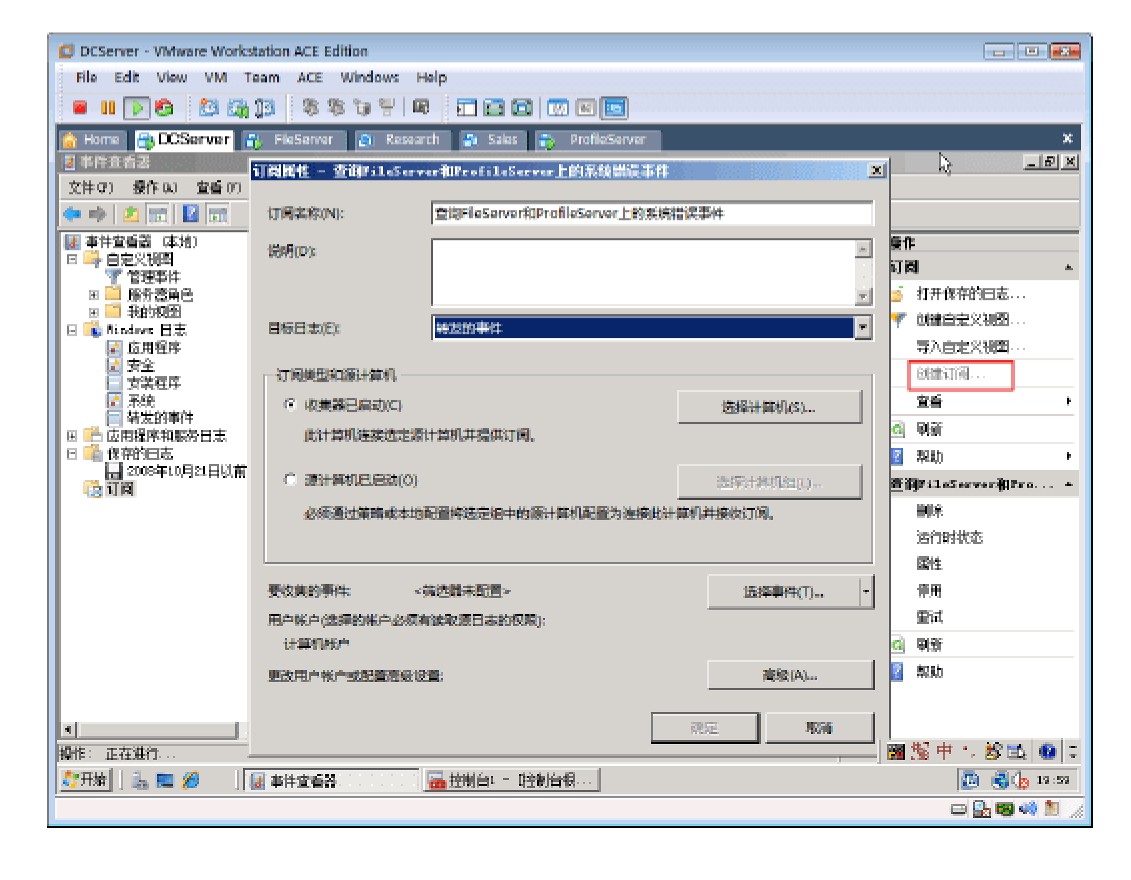


图 8-15　订阅其他计算机上的日志

⑱ 如图 8-16 所示，单击“选择计算机”按钮，在出现的“计算机”对话框中，单击“添加域计算机”按钮，输入 ProfileServer 和 FileServer 计算机，单击“确定”按钮。

⑲ 如图 8-17 所示，单击“选择事件”按钮，记录时间为“最后 7 天”，事件级别选中“错误”和“警告”，事件日志选择“系统”。单击“确定”按钮。

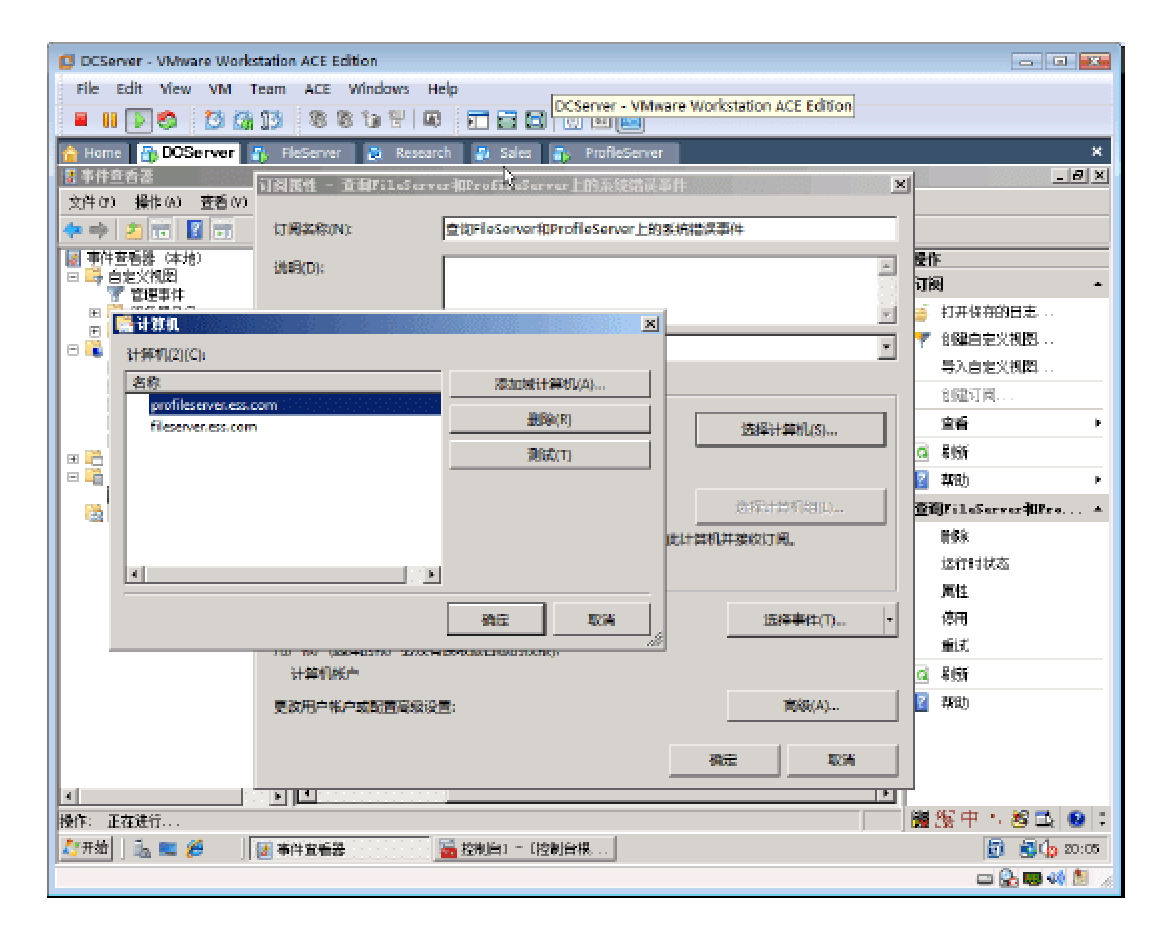


图 8-16　选择计算机

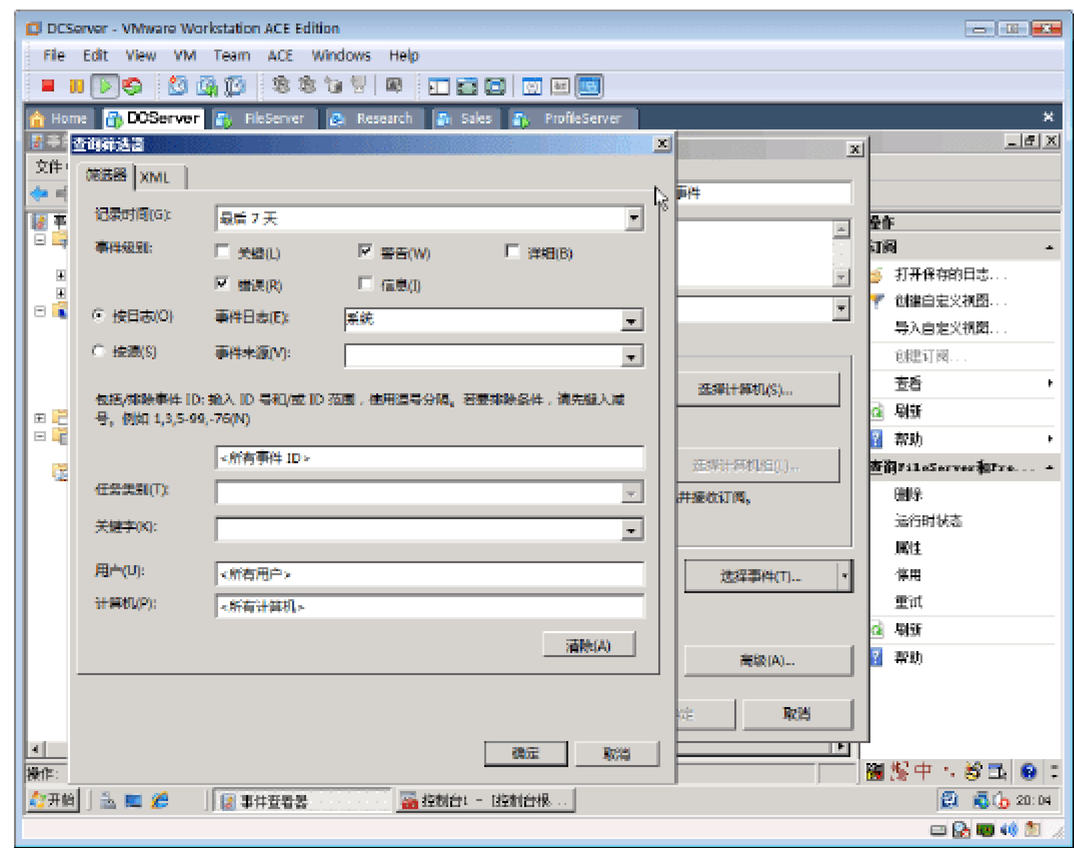


图 8-17　选择订阅的日志

⑳　如图 8-18 所示，展开“Windows 日志”→“转发的事件”节点。此时，可以看到订阅的 ProfileServer 和 FileServer 计算机上的系统日志。

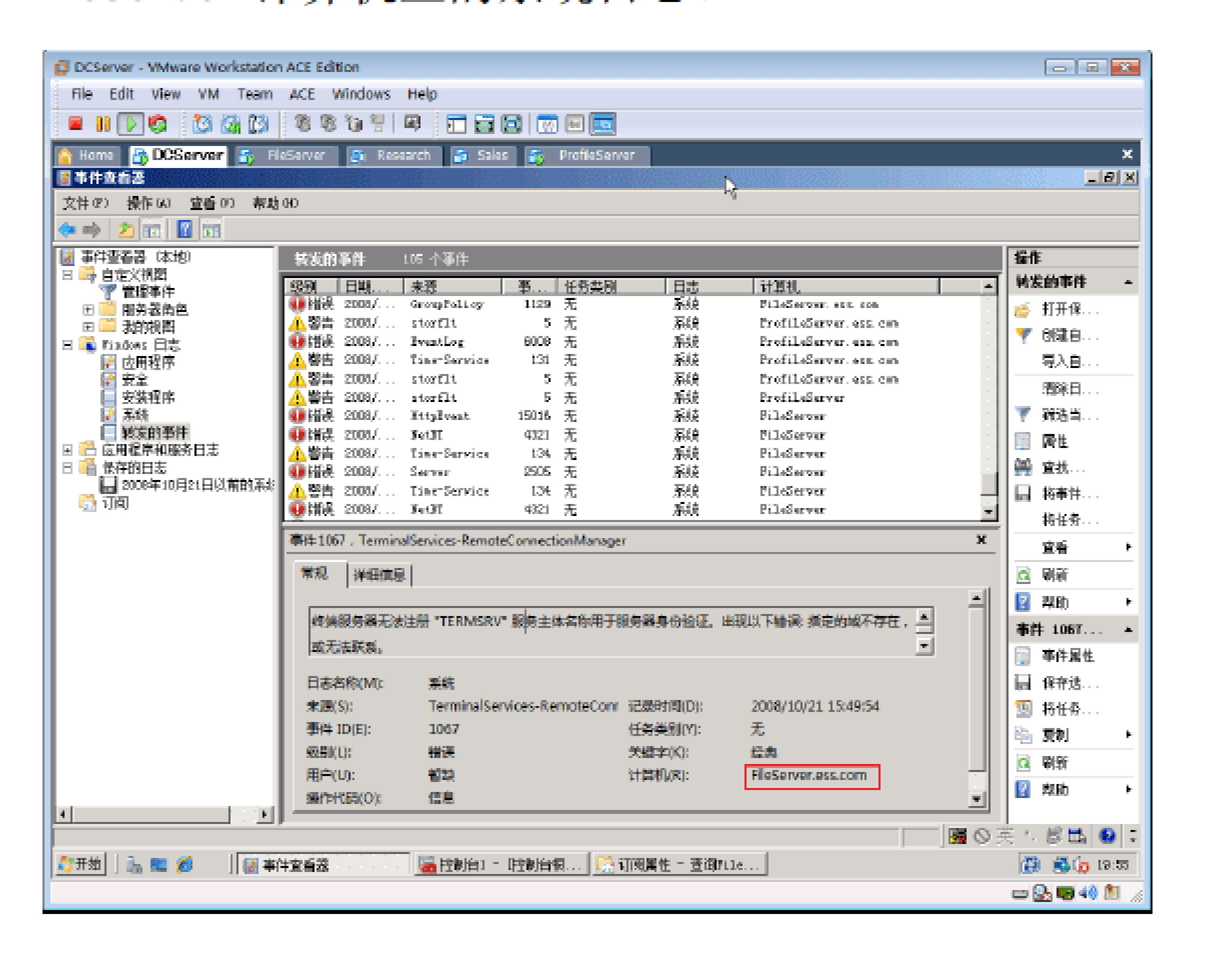


图 8-18　查看订阅的其他服务器的日志

8.2　利用任务管理器监控系统资源

任务管理器显示计算机上当前正在运行的程序、进程和服务。可以使用任务管理器监视计算机的性能或者关闭没有响应的程序。

如果你与网络连接，还可以使用任务管理器查看网络状态以及你的网络是如何工作的。如果有多个用户连接到你的计算机，你可以看到他们是谁、在做什么，还可以给他们发送消息。

8.2.1　实时检测内存和 CPU 的使用情况

①　可以通过右击任务栏上的空白区域打开任务管理器，然后选择“任务管理器”命令，或者通过按

Ctrl+Shift+Esc 组合键来打开任务管理器，如图 8-19 所示。

② 切换到任务管理器的“性能”选项卡，可以看到 CPU 和内存的使用情况。

③ 选择“查看”→“显示内核时间”命令。在图标中，处于内核模式的处理器时间用红色显示，它就是应用程序正在使用操作系统服务的时间量。其余的时间用绿色显示，并被称为“用户模式”。它就是在应用程序的代码内用于运行线程的时间量。

④ 单击“资源监视器”按钮，打开如图 8-20 所示的对话框，可以看到 CPU、硬盘、网络和内存的使用情况。可以看到那个进程正在读写磁盘。

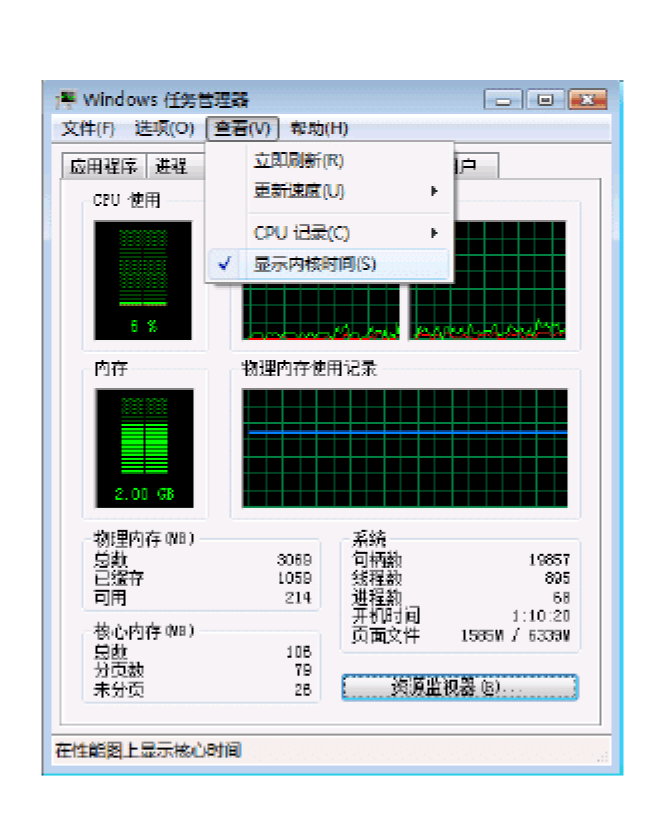


图 8-19　实时查看内存和 CPU 的使用情况

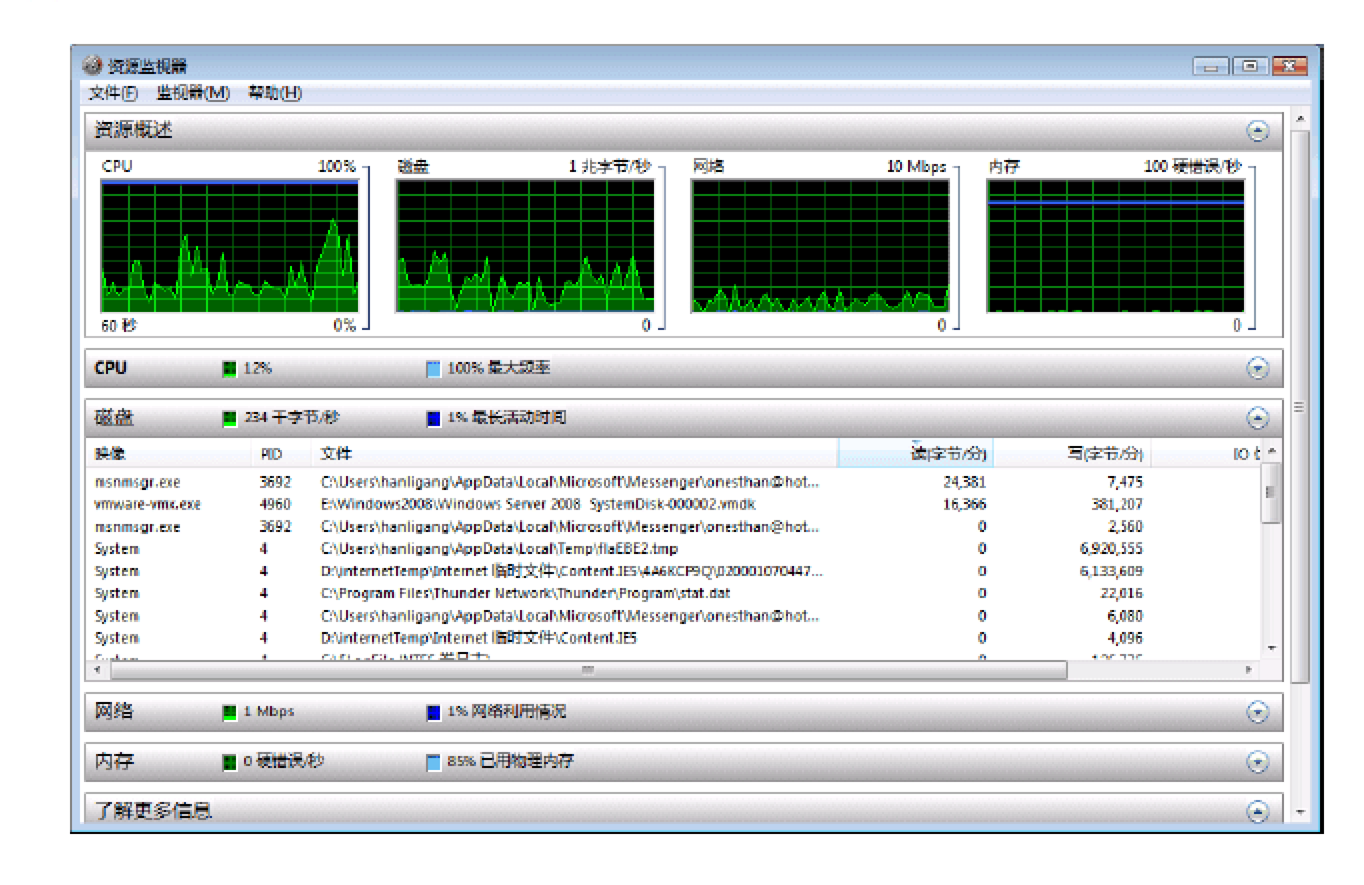


图 8-20　资源监视器

8.2.2　退出没有响应的程序

如果计算机中的程序停止响应，则 Windows 将尝试查找问题并自动解决该问题。如果你不想等待，则可以使用任务管理器自己结束该程序。

使用任务管理器结束程序可能比等待更快，但是将丢失所有未保存的更改。如果你想保留重要的工作，则等待几分钟，首先让 Windows 尝试解决该问题。

如图 8-21 所示，打开任务管理器。切换到“应用程序”选项卡，单击未响应的程序，然后单击“结束任务”按钮。

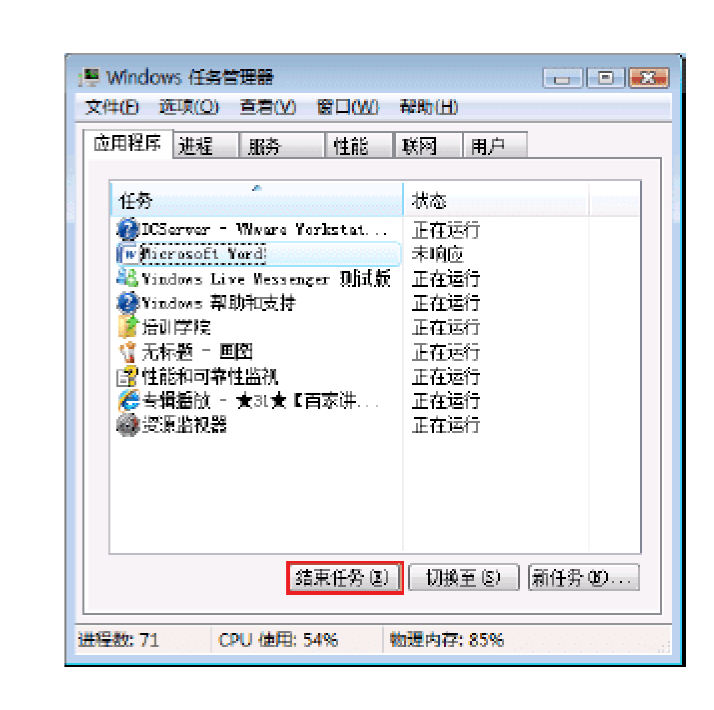


图 8-21　结束不响应的程序

8.2.3　识别与程序关联的进程

可以查看应用程序的进程，如图 8-22 所示，右击选中的应用程序，在弹出的快捷菜单中选择“转到进程”命令。

如图 8-23 所示，可以看到该应用程序对应的进程。也可以通过结束进程来结束应用程序。

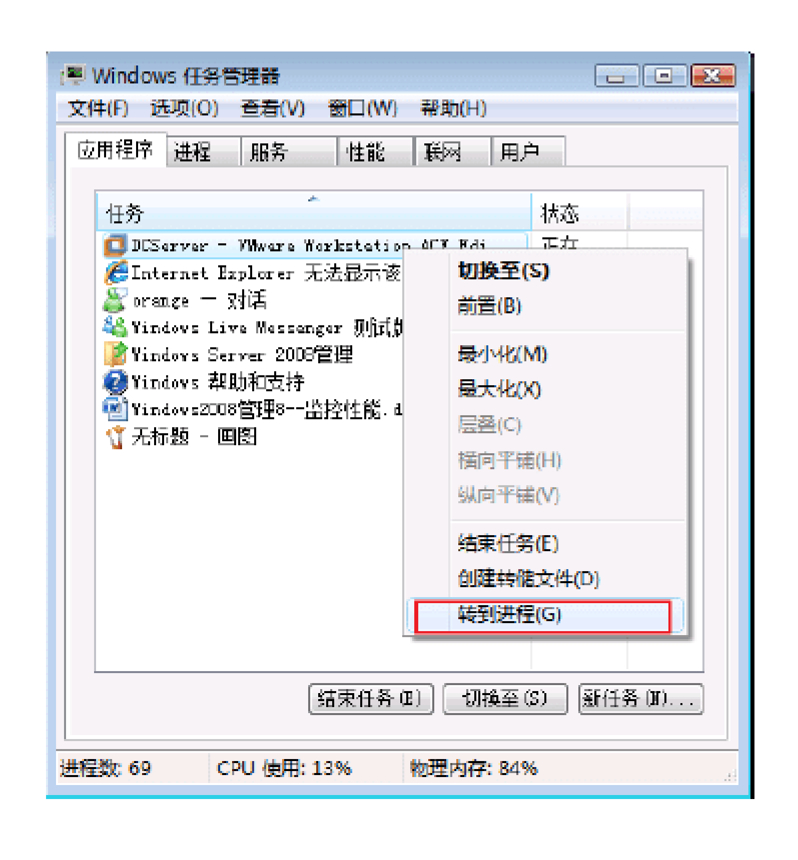


图 8-22　转到程序的进程

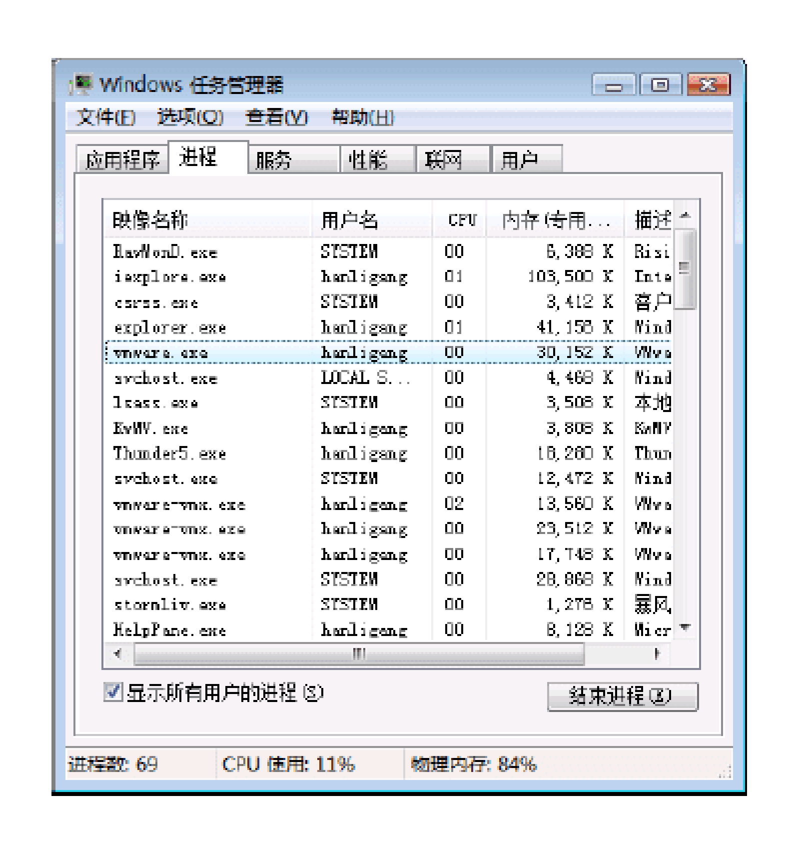


图 8-23　查看程序的进程

8.2.4　添加监控的列

在任务管理器的“进程”选项卡中，可以添加你关心的其他性能指标。

在“Windows 任务管理器”的“查看”菜单中有一个“选择列”命令，列出了可选的一些反映进程运行情况的参数。下面列出常用的进程量度数据。

- PID 进程标识符号：每个进程都有一个数字号；这个号码与它所指定的进程是完全等价的，就像身份证号码同我们自己的关系一样。
- CPU 使用和时间：CPU 时间是表明一个进程自启动以来所占用 CPU 时间的总和；CPU 使用是指一个进程占用 CPU 的百分比。
- 内存使用增量：是指进程使用内存的变化。正值表示增加，负值表示减少。
- 内存使用高峰期：是指一个进程自启动以来使用的最大内存值。
- 页面错误：当软件试图读写标有不存在的虚拟内存地址时，中断发生了。页面错误记录了一个进程必须从硬盘上恢复的次数。
- 虚拟内存大小：是给一个进程安排的虚拟内存的大小或地址空间。
- 内存——页面缓冲池：系统分配给一个进程的虚拟内存，它是可以分页的。分页是指把进程的不常使用的工作内存从 RAM 移至硬盘。
- 基本优先级：是一个处理排名，它确定了一个进程中的线程被处理的顺序。
- I/O 读取和 I/O 读取字节：I/O 读取是指一个进程产生的读输入/输出操作的个数，包括文件个数、网络个数和输入/输出设备个数。而 I/O 读取字节是指相应的字节数。
- I/O 写入和 I/O 写入字节：I/O 写入是指一个进程产生的写输入/输出操作的个数，包括文件个数、网络个数和输入/输出设备个数。而 I/O 写入字节是指相应的字节数。
- I/O 其他和 I/O 其他字节：I/O 其他是指一个进程产生的非读非写输入/输出操作的个数，包括文件个数、网络个数和输入/输出设备个数。而 I/O 其他字节是指相应的字节数。

在“进程”选项卡中，如图 8-24 所示，选择“查看”→“选择列”命令。

如图 8-25 所示，选中“CPU 时间”、“I/O 读取”和“I/O 写入”复选框，单击“确定”按钮。

如图 8-28 所示，可以看到各个进程使用 CPU 的累计时间。

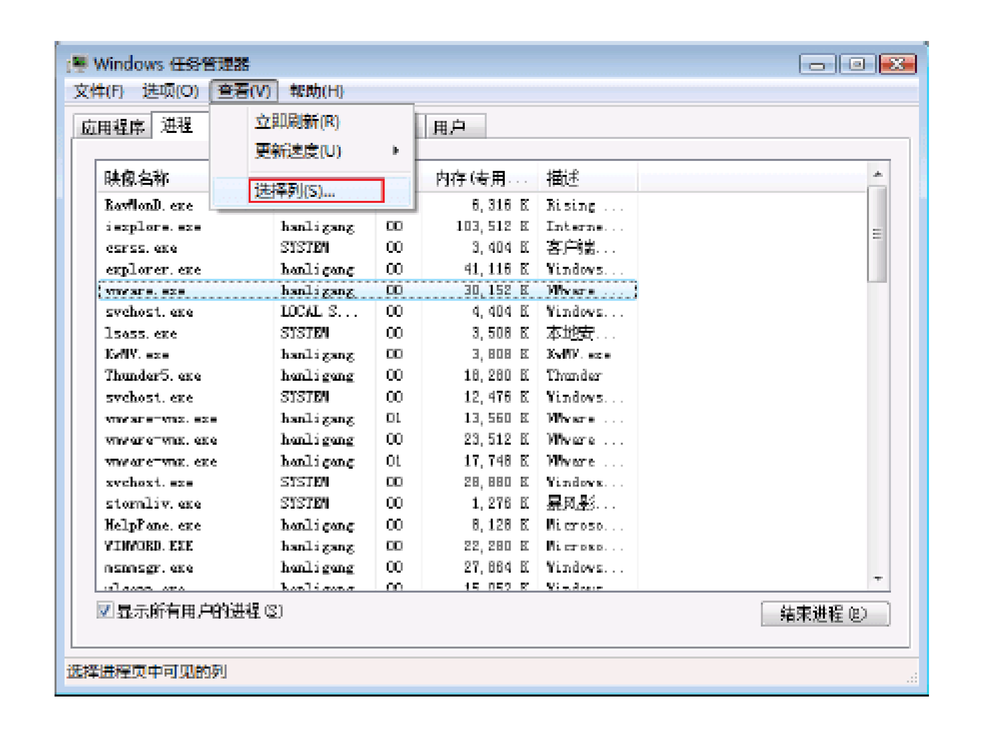


图 8-24　选择列

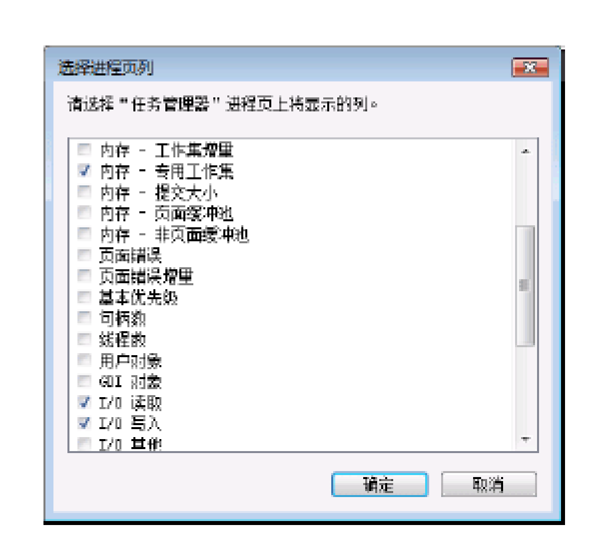


图 8-25　选择显示的列

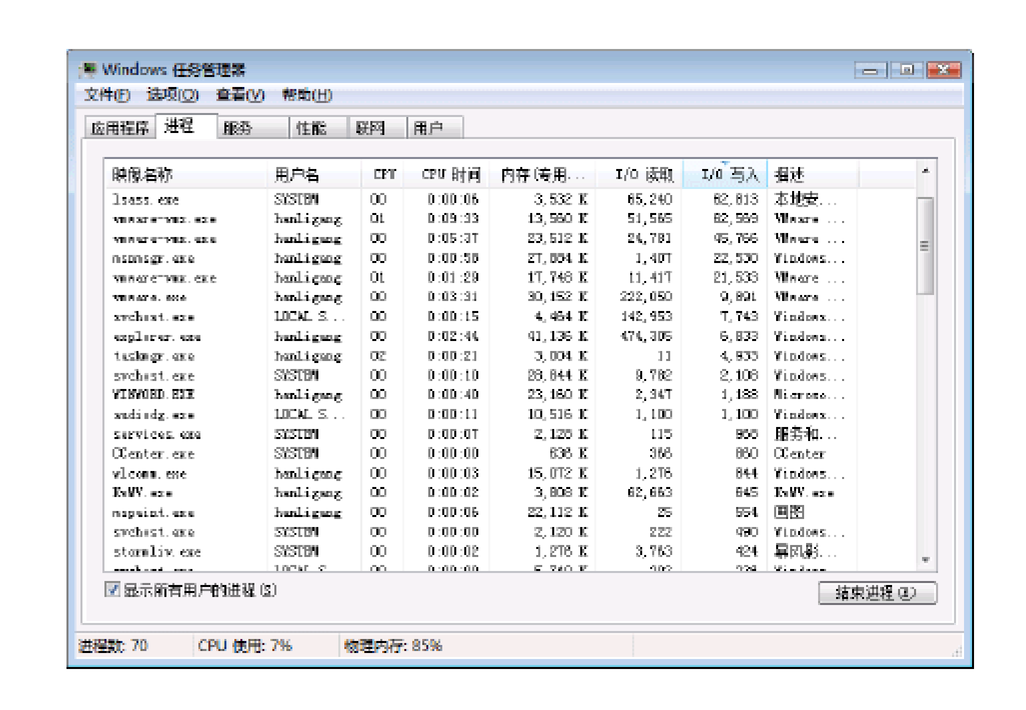


图 8-26　查看添加的列

8.2.5　排序进程

打开 Windows 任务管理器，如图 8-27 所示，切换到“进程”选项卡，单击“内存”列，可以按内存的使用排序进程，能够看到哪些进程使用内存较多。

如图 8-28 所示，单击 CPU，可以按 CPU 的使用情况排序进程。通过排序，可以识别程序对资源的使用情况。如果你识别出来某些应用程序占用了大量的处理器时间，可以将其中的某些应用程序移动到另外一个计算机上，用于适当分配工作负荷。

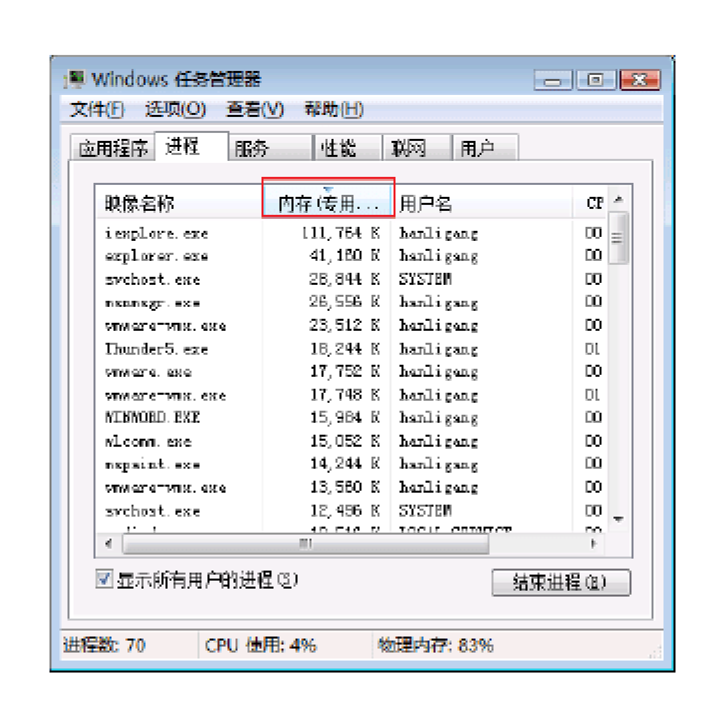


图 8-27　按内存的使用大小排序

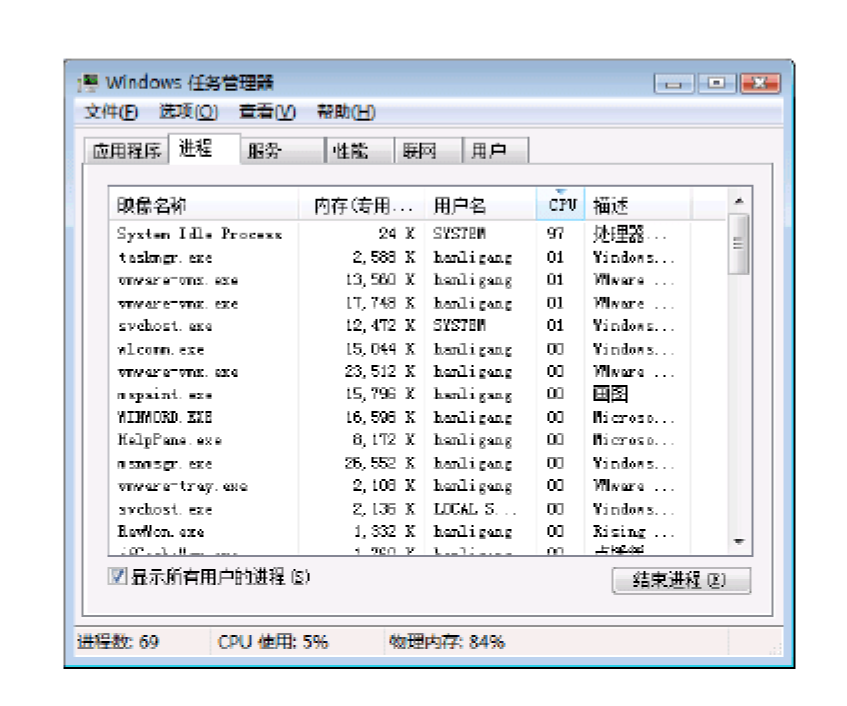


图 8-28　按 CPU 使用排序

8.3 利用“性能监视器”检测系统性能

Windows 可靠性和性能监视器使用可合并进数据收集器的性能计数器、事件来跟踪数据和配置信息。

8.3.1 使用性能监视器实时监控

“性能计数器”是系统状态或活动情况的量度单位。它们可以包含在操作系统中或作为个别应用程序的一部分。Windows 可靠性和性能监视器以指定的时间间隔请求性能计数器的当前值。

示例：监控磁盘读写情况。

① 选择“开始”→“程序”→“管理工具”→“可靠性和性能监视器”命令，打开性能监视器，如图 8-29 所示。

② 单击按钮，添加计数器，打开“添加计数器”对话框，单击 PhysicalDisk 下的 Disk Transfers/sec 和 Current Disk Queue Length。

- Disk Transfers/sec：指在此盘上读取/写入操作速率。
- Current Disk Queue Length：是在收集性能数据时磁盘上当前的请求数量。它还包括在收集时处于服务的请求。这是瞬间的快照，不是时间间隔的平均值。多轴磁盘设备能有一次处于运行状态的多重请求，但是其他同期请求正在等待服务。此计数器会反映暂时的高或低的队列长度，但是如果磁盘驱动器被迫持续运行，它有可能一直处于高的状态。请求的延迟与此队列的长度减去磁盘的轴数成正比。为了提高性能，此处应该平均小于 2。

③ 如图 8-30 所示，单击“显示描述”按钮，可以看到计数器的作用。

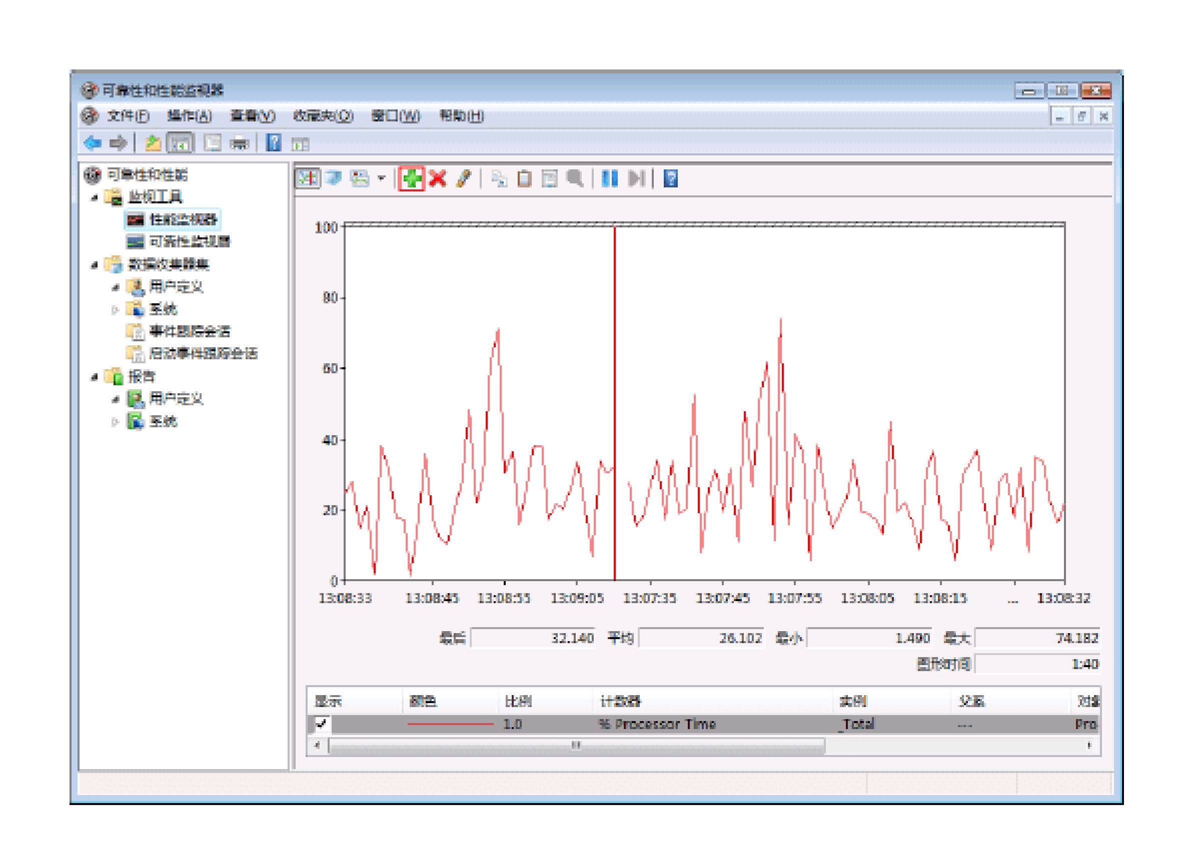


图 8-29 打开性能监视器

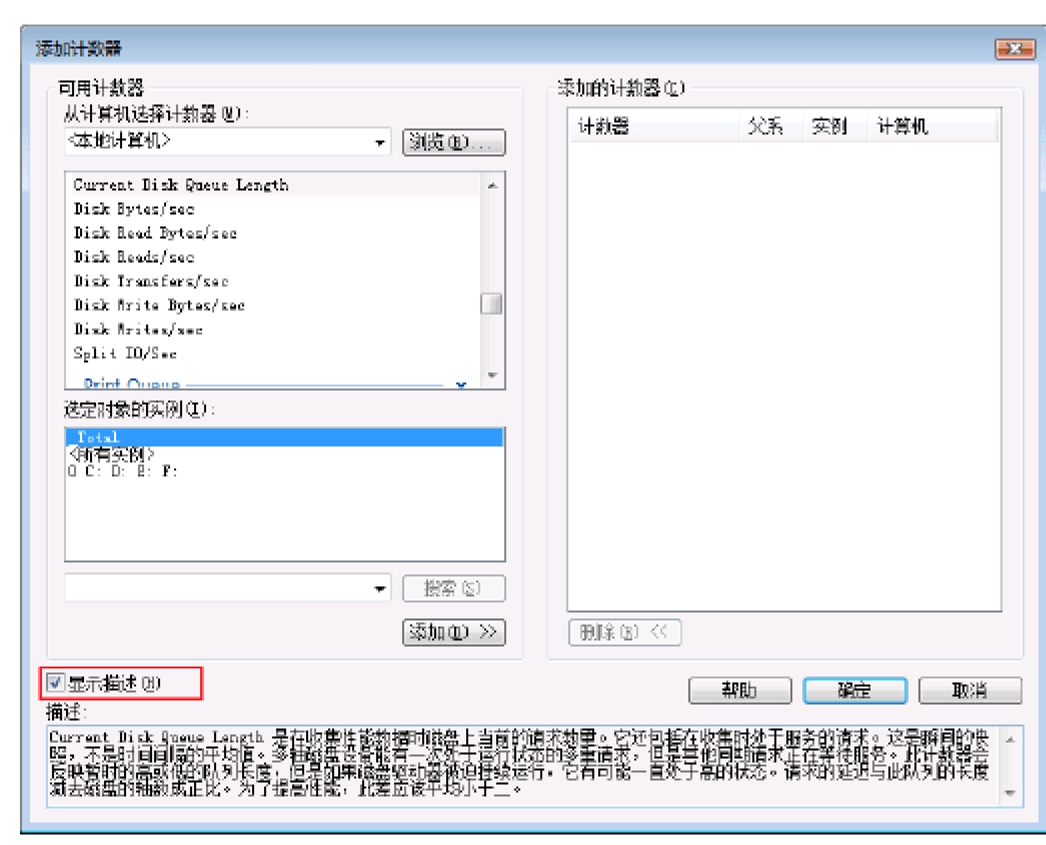


图 8-30 显示计数器描述

④ 此时，可以实时观察每个计数器的值，单击按钮，可以选择直方图条或报告的形式观察计数器的值，如图 8-31 所示。

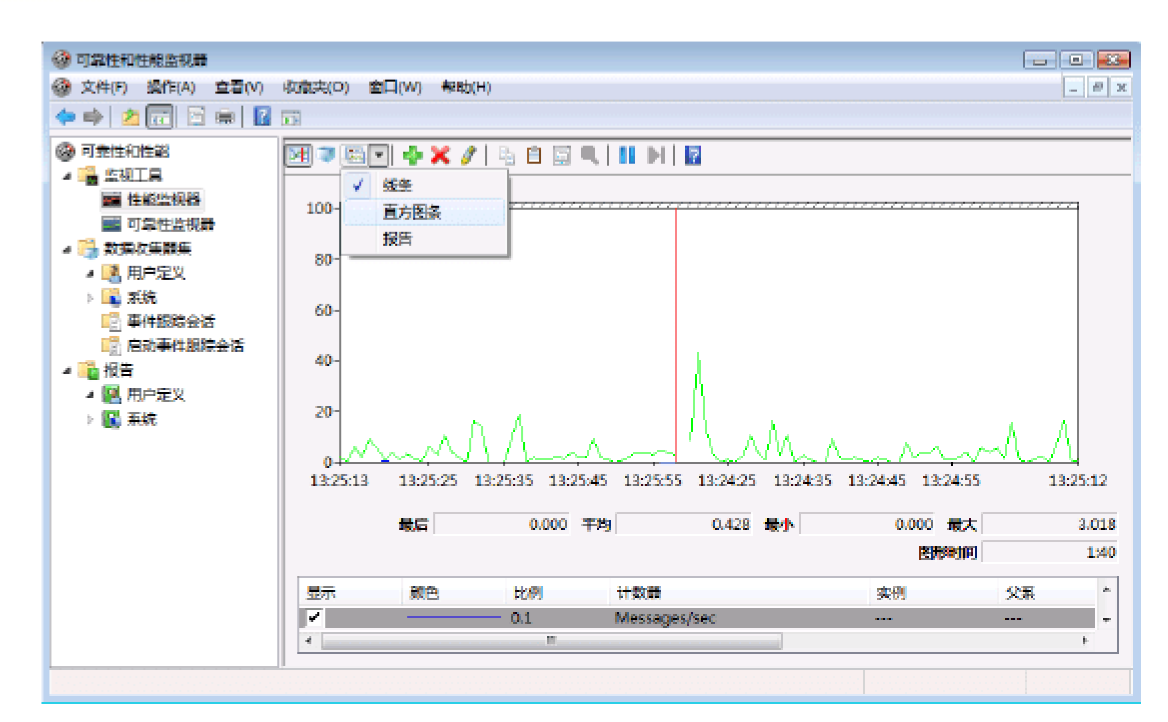


图 8-31　改变显示方式

8.3.2　监控远程计算机的性能

你可以远程监控计算机的性能，只要你有访问远程计算机管理员权限。

在域环境中域管理员默认是所有域中成员计算机的管理员组的成员，因此以域管理员账户登录，能够远程监控域中计算机的性能。

要想远程监控工作组中的远程计算机，需要访问远程计算机的共享文件，输入远程计算机的管理员账号和密码，这样你的计算机就缓存了访问远程计算机的凭据。或依次单击(或选择)“控制面板”→“用户账户”→“管理网络密码”，在打开的对话框中添加访问远程计算机的凭据。

如图 8-32 所示，在“添加计数器”对话框中，计算机可以输入远程计算机的 IP 地址，或计算机名。

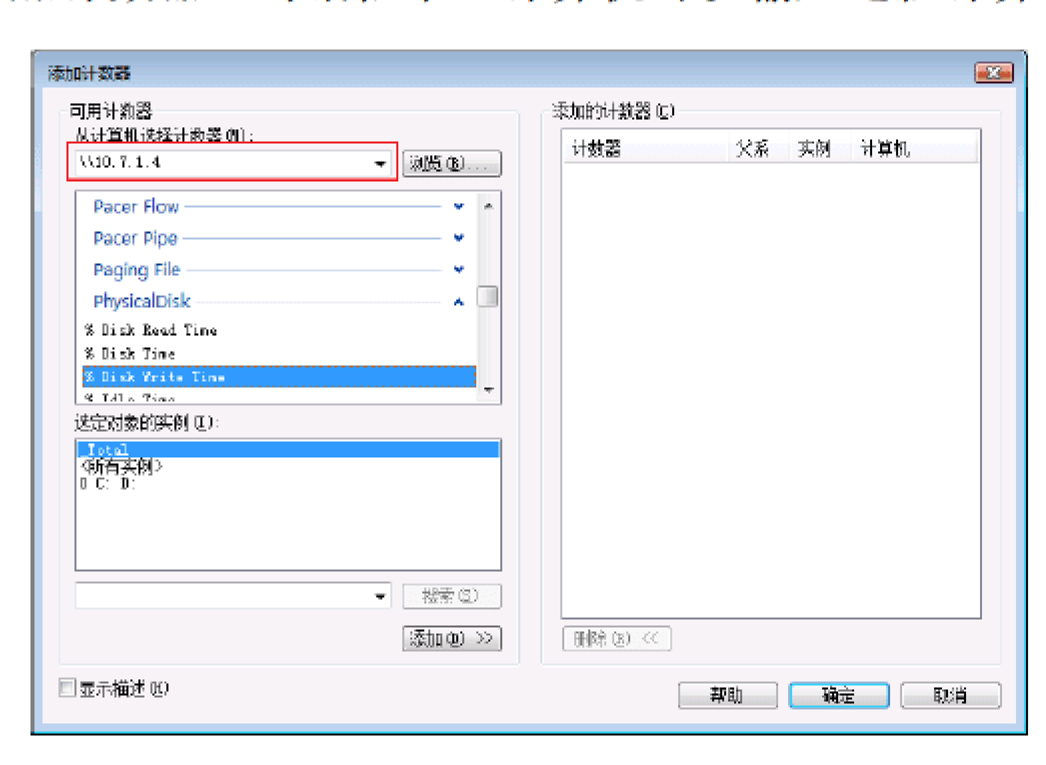


图 8-32　监视其他服务器性能



注意：计算机名称或 IP 地址前要添加\\。

8.3.3　使用系统内置的数据收集器

“事件跟踪数据”是从跟踪提供程序收集到的，这些跟踪提供程序是操作系统或者用于报告操作或事件的个别应用程序的组件。多个跟踪提供程序的输出可合并进一个 trace session，例如资源视图用于显示实时 CPU、内存、磁盘和网络活动的“Windows 内核跟踪”。

跟踪完毕后，系统给出诊断报告，告诉你服务器的瓶颈是内存还是 CPU、硬盘或网络。

示例：启用系统内置跟踪。

① 选择“开始”→“程序”→“管理工具”→“可靠性和性能监视器”命令。

② 打开如图 8-33 所示对话框，展开“数据收集器集”→“系统”节点，右击“System Performance(系统性能)”，在弹出的快捷菜单中选择“开始”命令。

③ 如图 8-34 所示，展开“报告”→System Performance 节点，单击最新的报告。可以看到 CPU、内存、网络和磁盘的性能计数器的值。

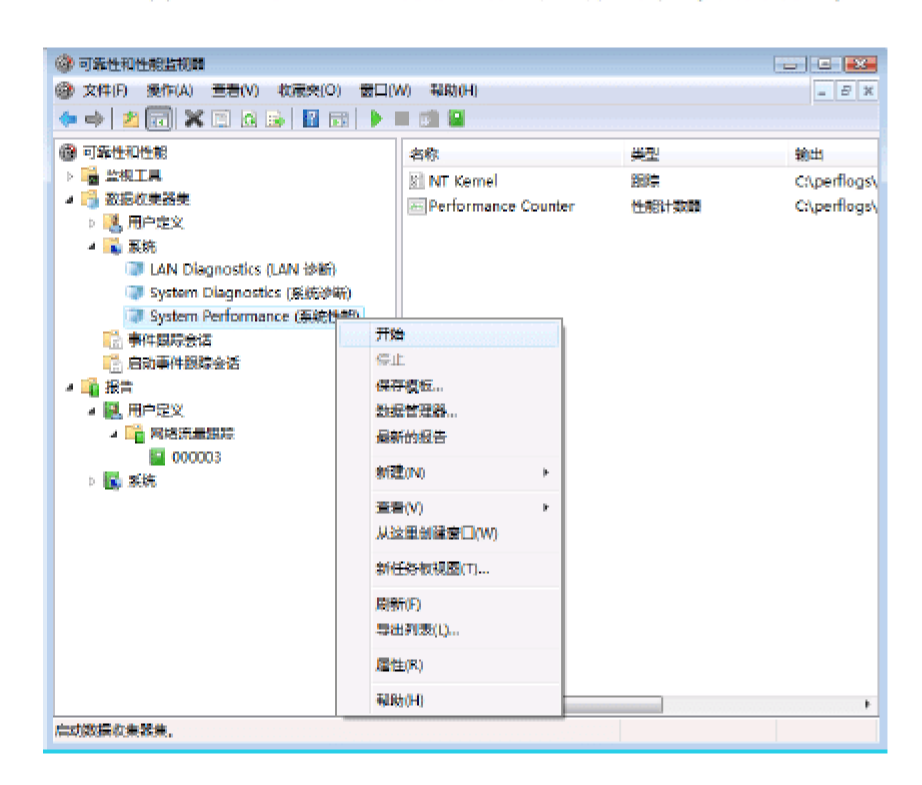


图 8-33　跟踪系统性能

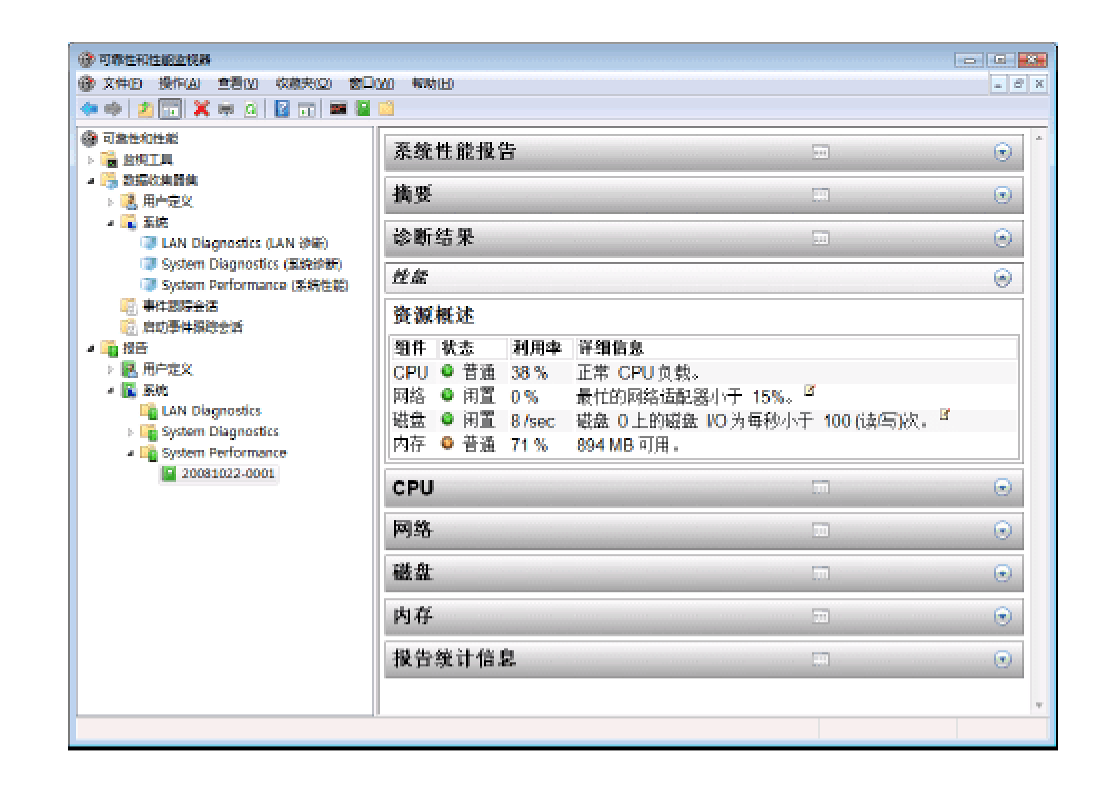


图 8-34　查看诊断报告

④ 如图 8-35 所示，单击图标，可以看到针对 CPU、内存、网络和磁盘的多种统计信息。

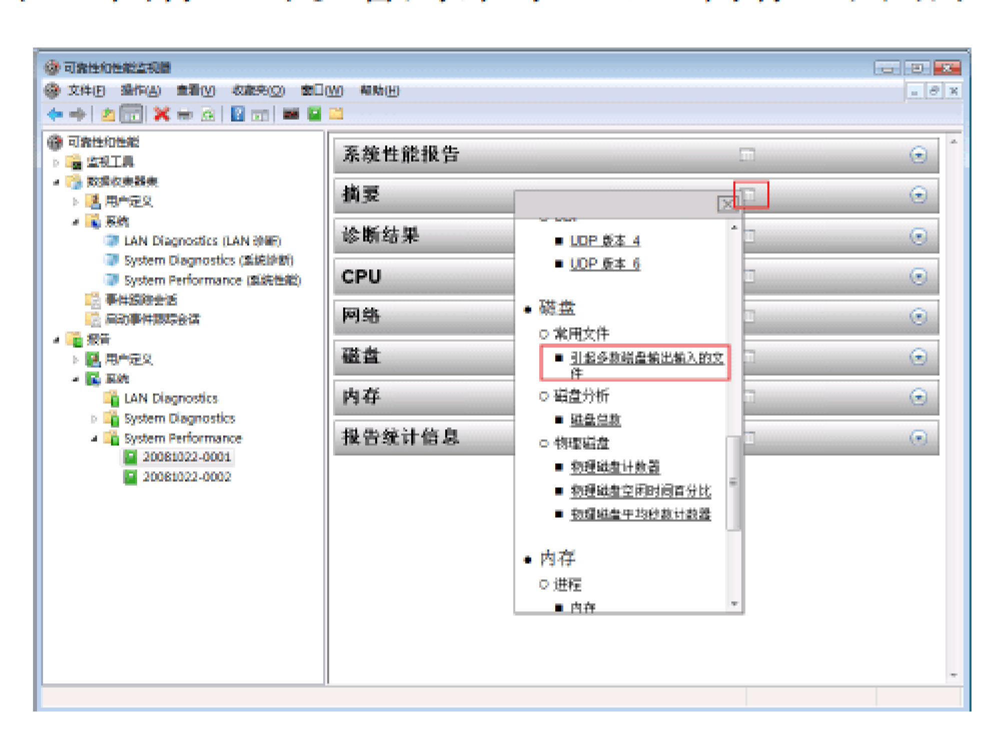


图 8-35　查看统计信息

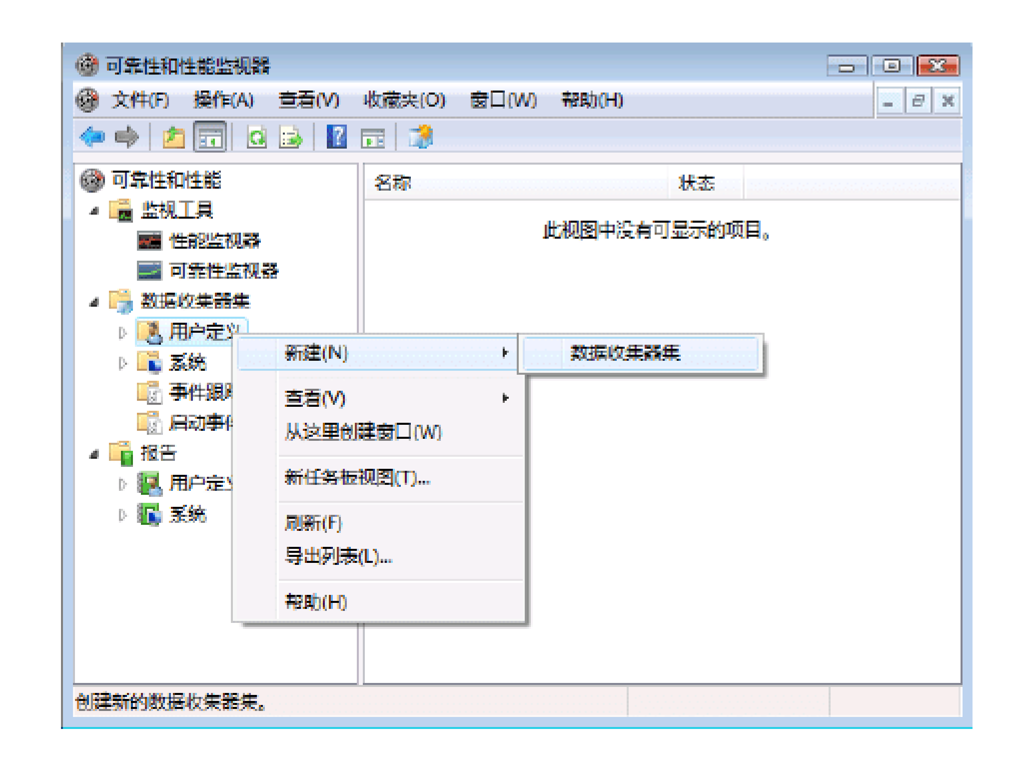
8.3.4　创建用户定义性能跟踪

可以创建自定义的数据收集器来跟踪所关注的性能指标。

示例：跟踪网络流量。

① 如图 8-36 所示，右击“数据收集器集”下的“用户定义”选项，在弹出的快捷菜单中，选择“新建”→“数据收集器集”命令。

② 如图 8-37 所示，在出现的“创建新的数据收集器集”对话框中，输入名称“网络流量跟踪”，选中“手动创建(高级)”单选按钮，单击“下一步”按钮。



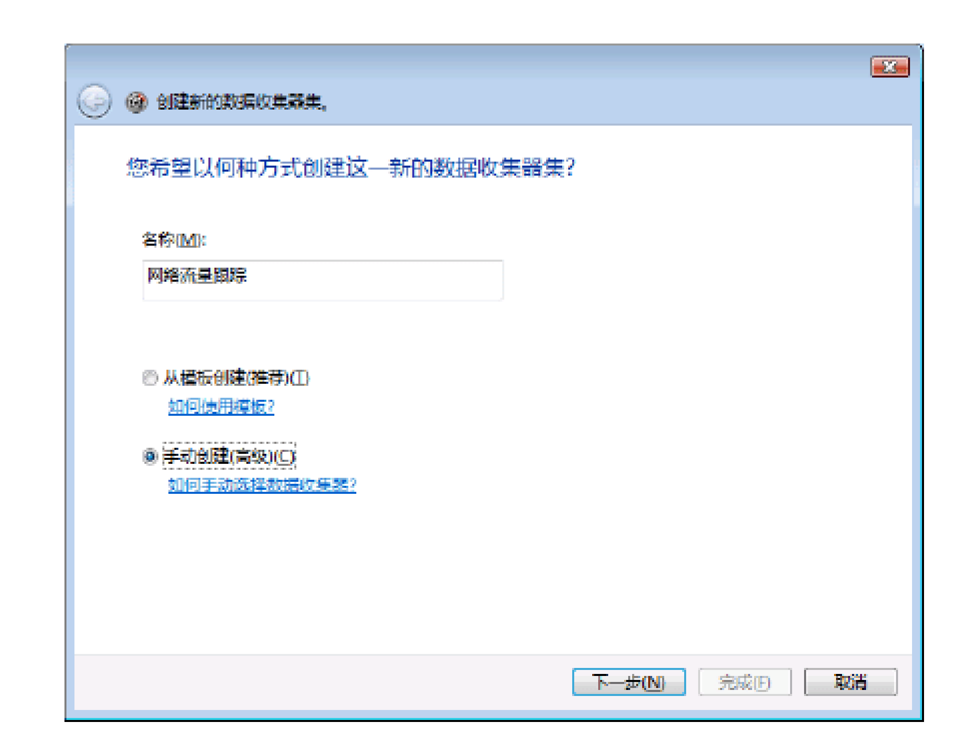


图 8-36　新建数据收集器集　　　　图 8-37　输入名称

③　如图 8-38 所示，在出现的“您希望包括何种类型的数据？”界面中，选中“性能计数器”复选框，单击“下一步”按钮。

④　如图 8-39 所示，在“您希望记录哪个性能计数器？”界面中，单击“添加”按钮。

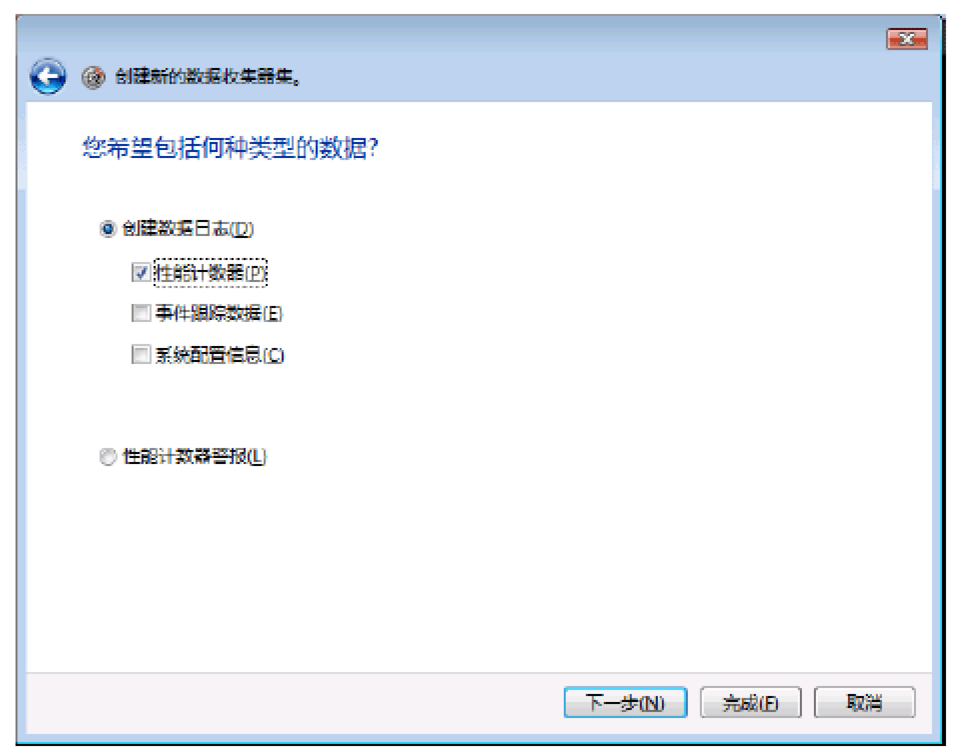
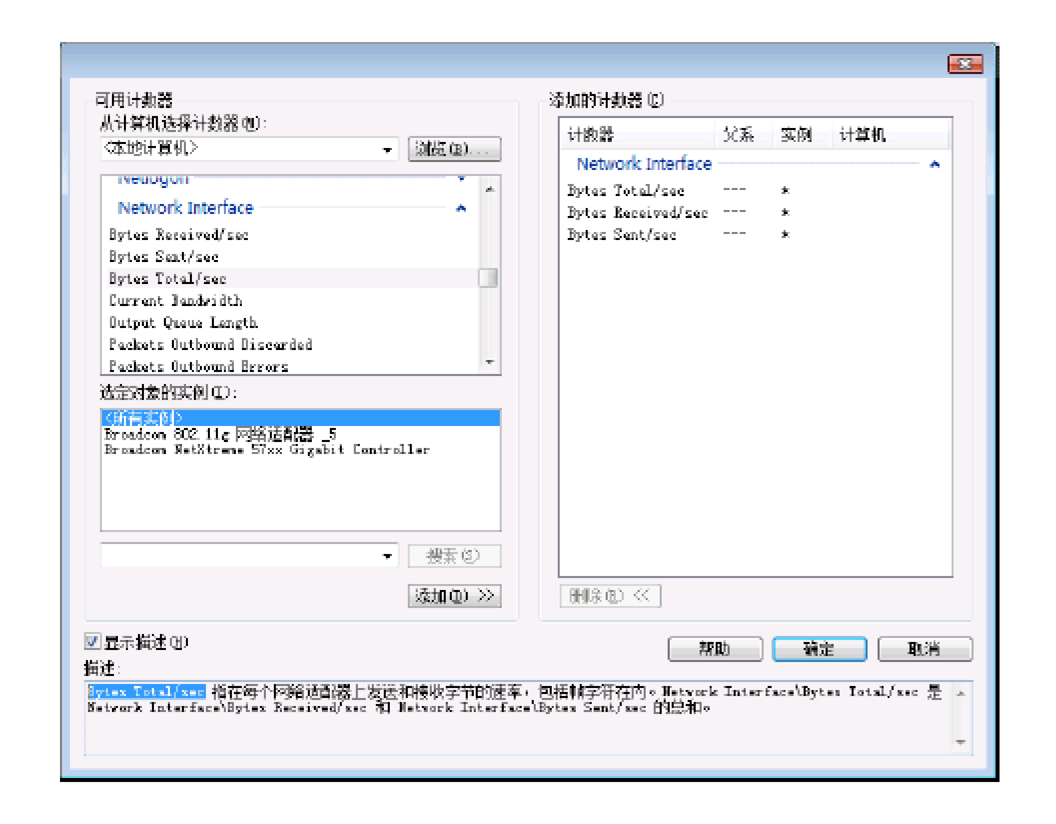


图 8-38　选中性能计数器　　　　图 8-39　添加性能计数器

⑤　如图 8-40 所示，在出现的“可用计数器”对话框中，选中 Network Interface 下的 Bytes Sent/sec、Bytes Received/sec 和 Bytes Total/sec，单击“确定”按钮。

⑥　如图 8-41 所示，更改“示例间隔”为 3 秒，单击“下一步”按钮。



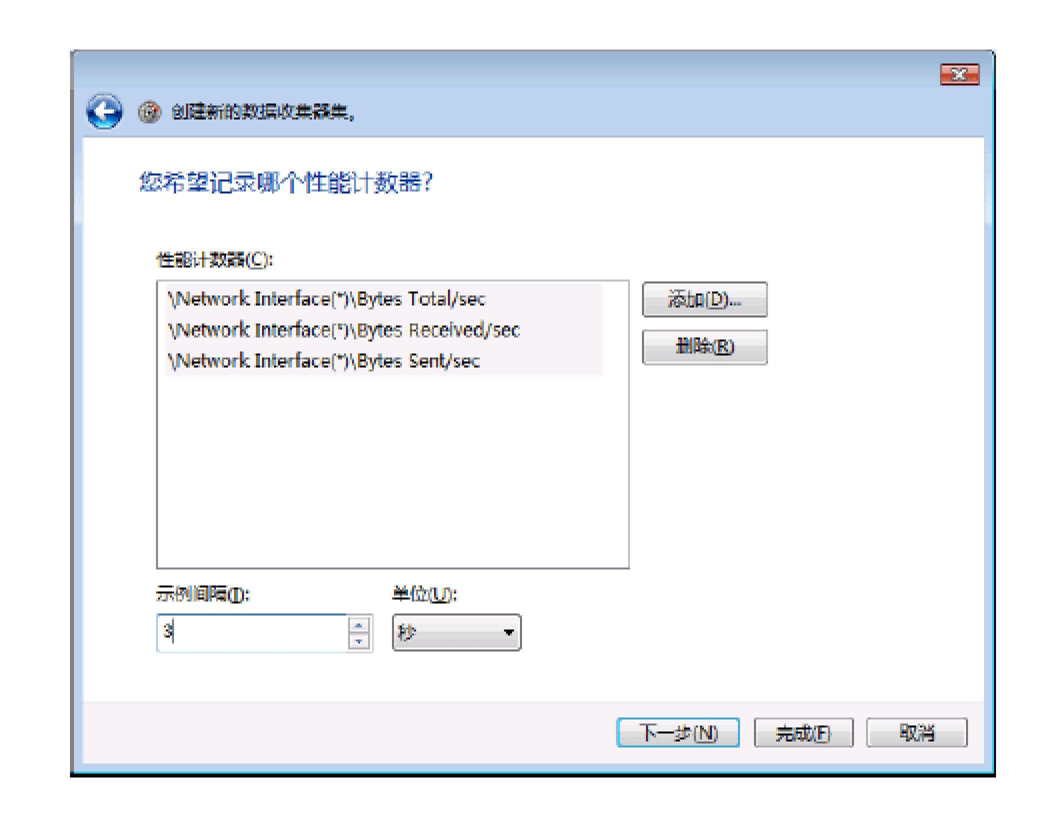


图 8-40　选择计数器实例　　　　图 8-41　选择计数器

⑦　如图 8-42 所示，在数据保存位置对话框中，保留默认位置，单击“下一步”按钮。

⑧　如图 8-43 所示，选中“立即启动该数据收集器集”单选按钮，单击“完成”按钮。

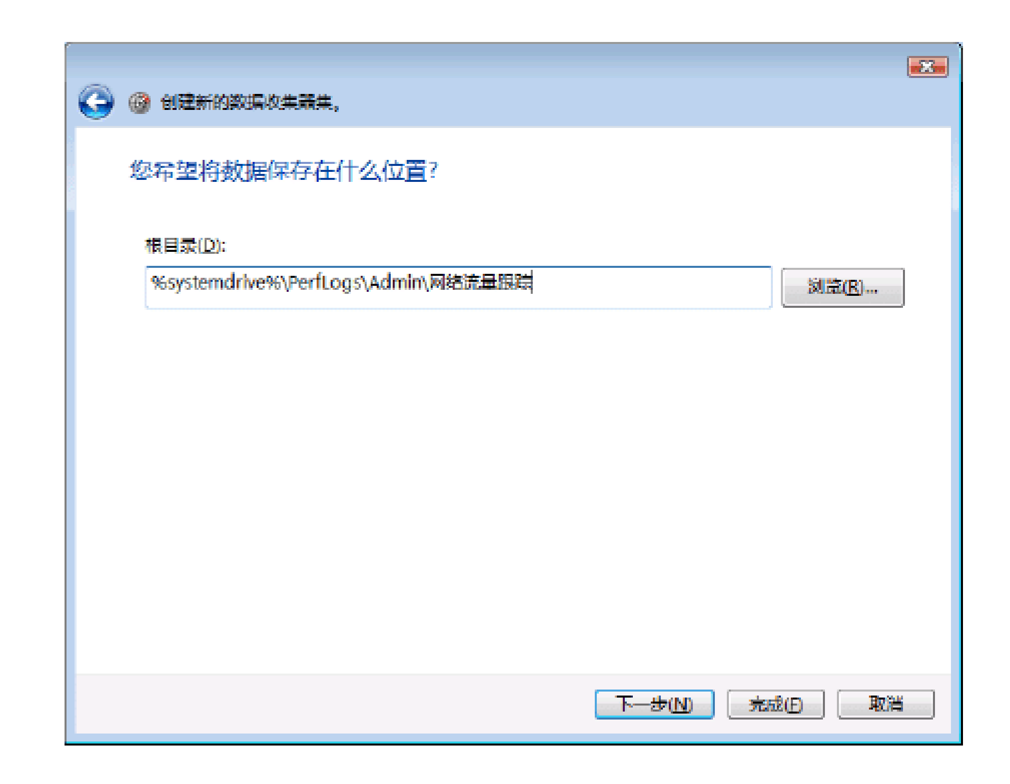


图 8-42　指定保存位置

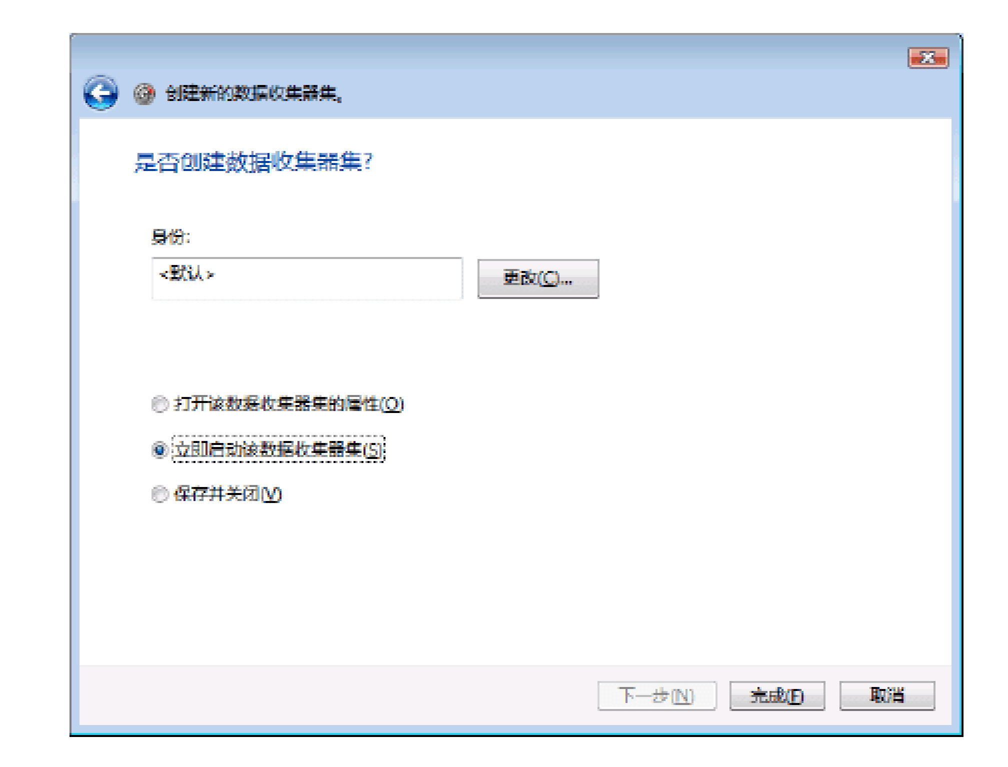


图 8-43　立即启动

⑨　如图 8-44 所示，依次展开“报告”→“用户定义”→“网络流量跟踪”节点，可以看到报告状态，正在收集数据。

⑩　如图 8-45 所示，选中刚才创建的“网络流量跟踪”，右击■图标，停止跟踪。

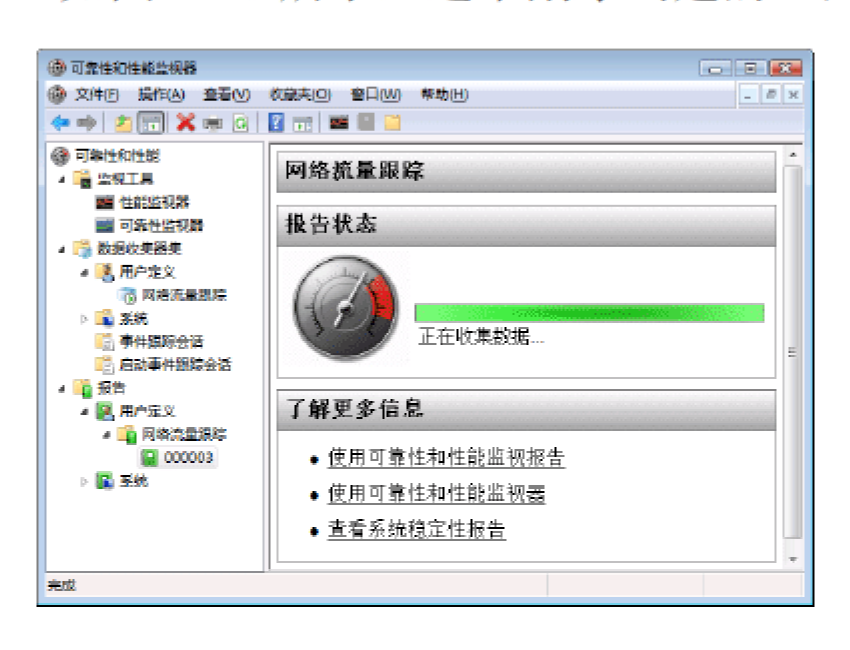


图 8-44　查看报告

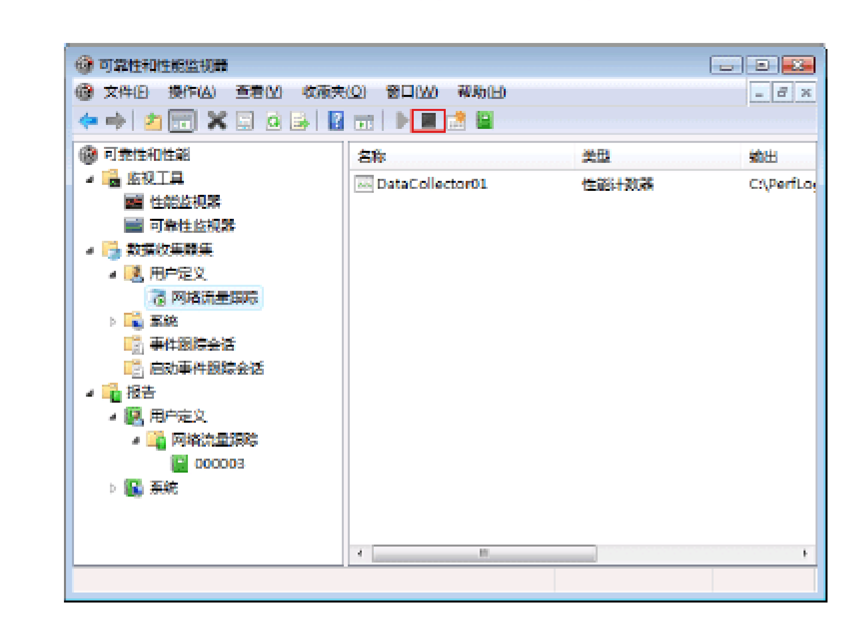


图 8-45　停止跟踪

⑪　如图 8-46 所示，依次展开“报告”→“用户定义”→“网络流量跟踪”节点，单击编号为 000003，单击✚。

⑫　如图 8-47 所示，在“添加计数器”对话框中，单击⌄，显示所有计数器，单击“添加”按钮，然后单击“确定”按钮。

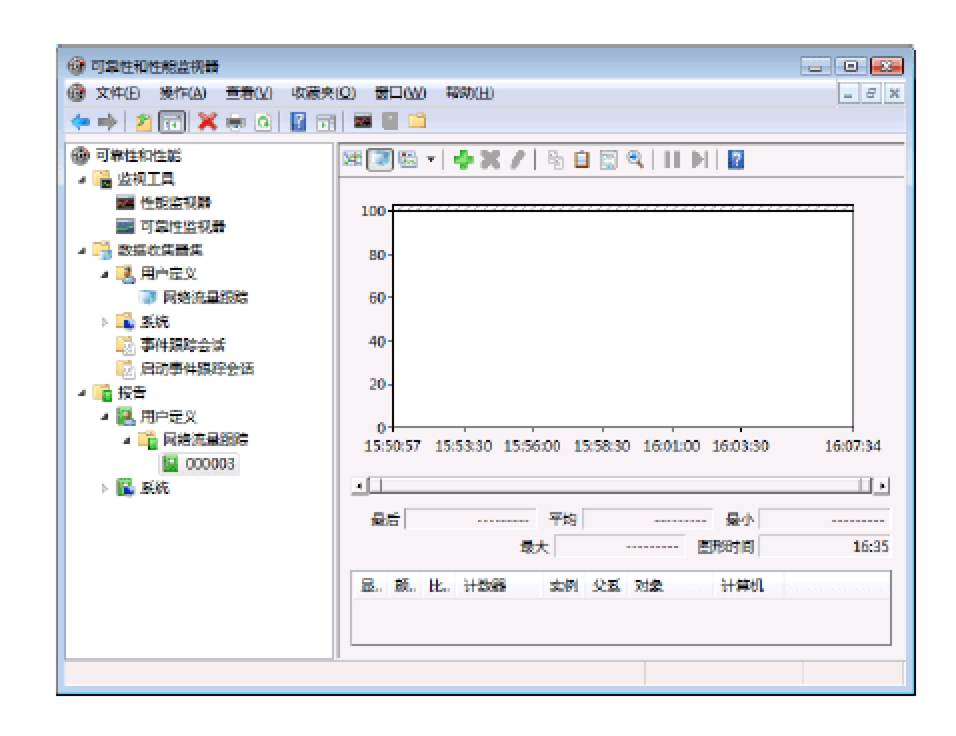


图 8-46　添加跟踪的计数器

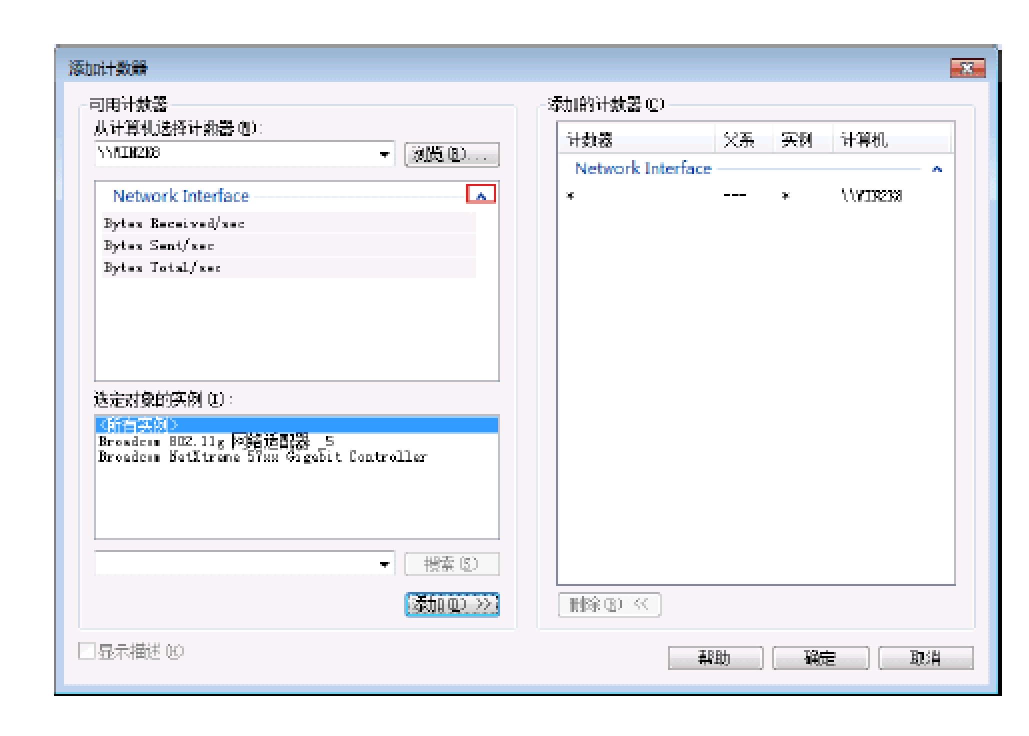


图 8-47　添加计数器

⑬　如图 8-48 所示，可以看到跟踪的结果。

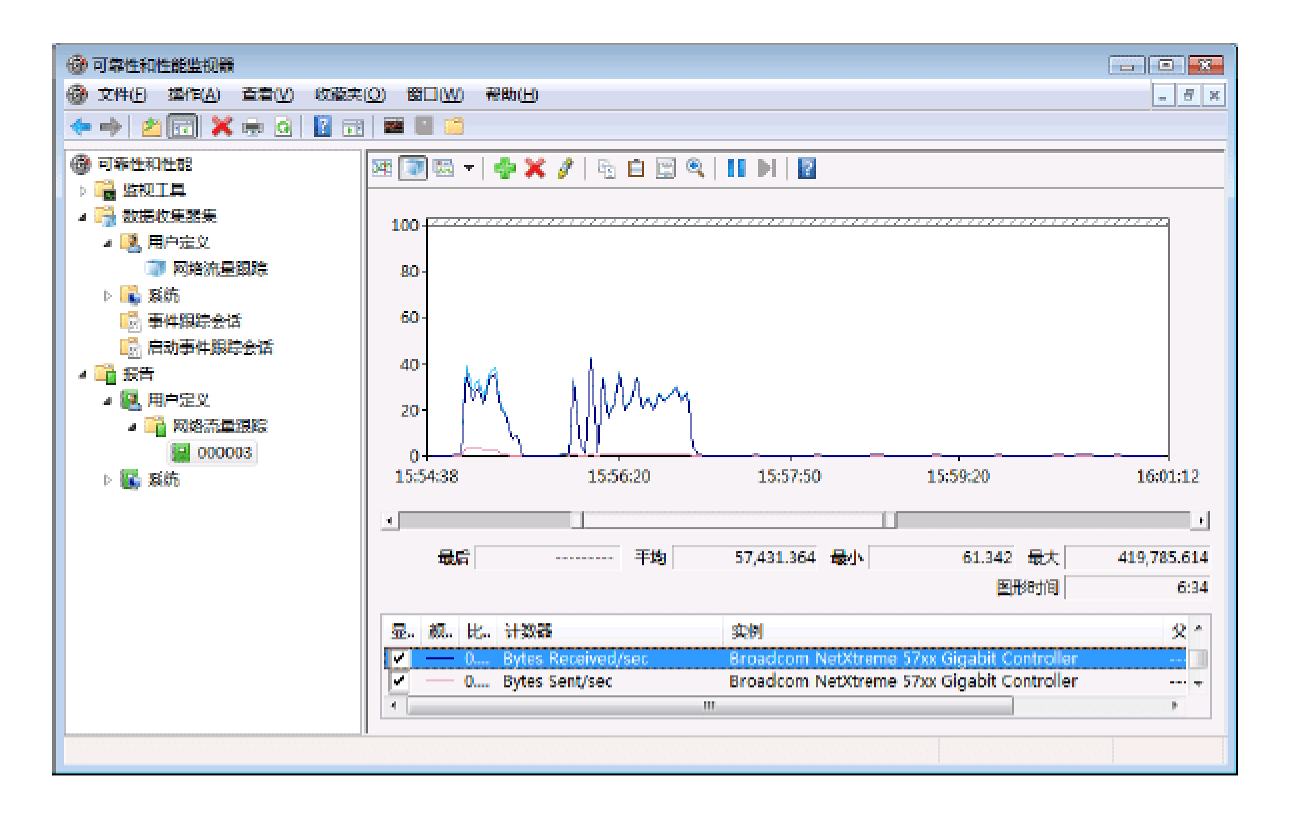


图 8-48　跟踪结果

8.3.5　指定数据收集计划

可以指定数据收集计划和停止条件。

如图 8-49 所示，右击“网络流量跟踪”，在弹出的快捷菜单中选择“属性”命令。在弹出的对话框的“计划”选项卡中，单击“添加”按钮，可以指定开始日期和截止日期，以及时间安排。

- 可以使用单个停止条件或组合使用多个条件来自动暂停或重新开始收集数据收集器集中的数据。
- 选中复选框以选择一个或所有要应用于数据收集器集的停止条件。如果在此选项卡中未选定停止条件，数据收集器集将从启动(手动或自动)时间开始收集数据，直到手动停止。
- “总持续时间”会使数据收集器集在超过配置时间之后停止收集数据。总持续时间设置优先于定义为限制的任何设置。
- “限制”可用于代替总持续时间停止条件，或与其一起使用。

如图 8-50 所示，若要在达到持续时间、大小的限制或同时达到这两种限制时自动重新开始数据收集器集的收集操作，请选中复选框。当与总持续时间停止条件组合使用时，配置自动重新开始会使每个指定时间段或大小的数据收集到单独的日志文件中，直到满足总持续时间停止条件。

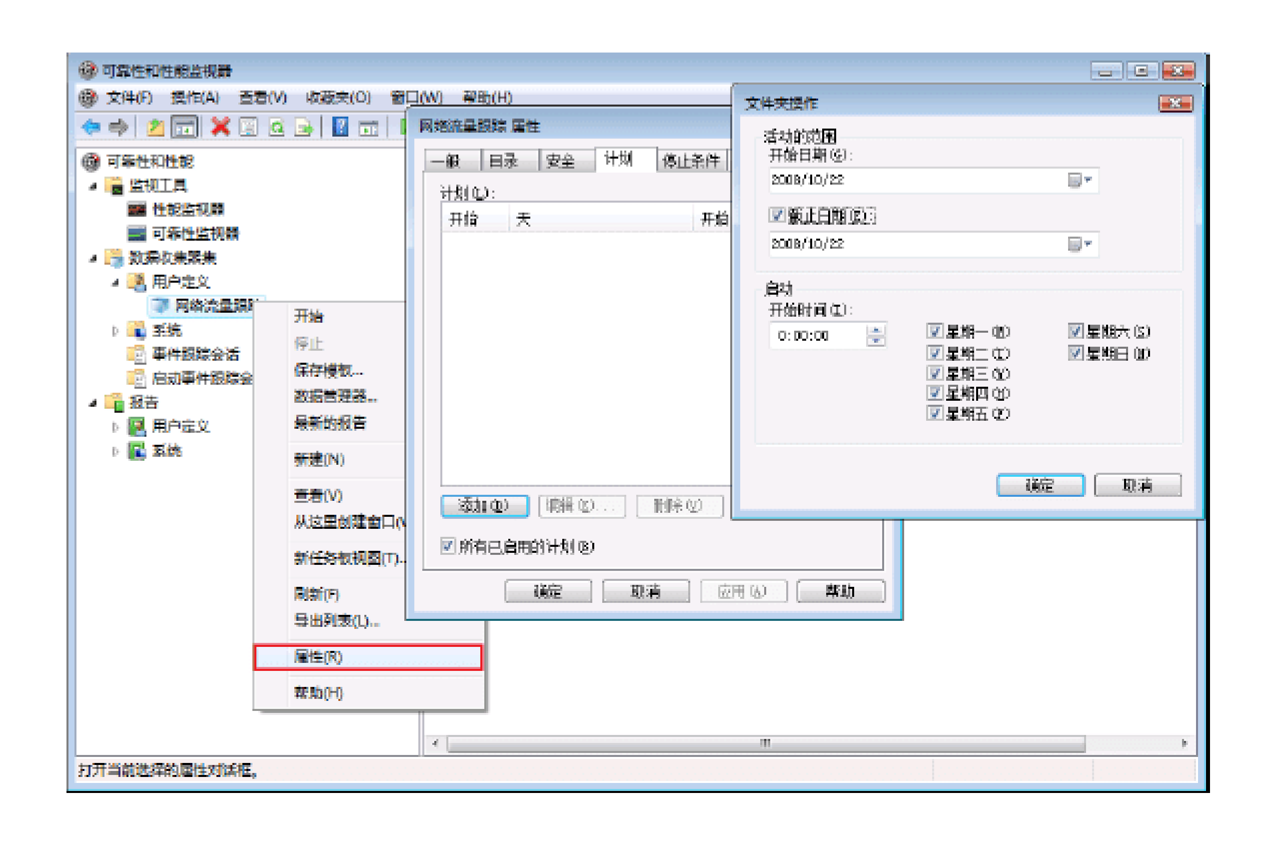


图 8-49　指定数据收集计划

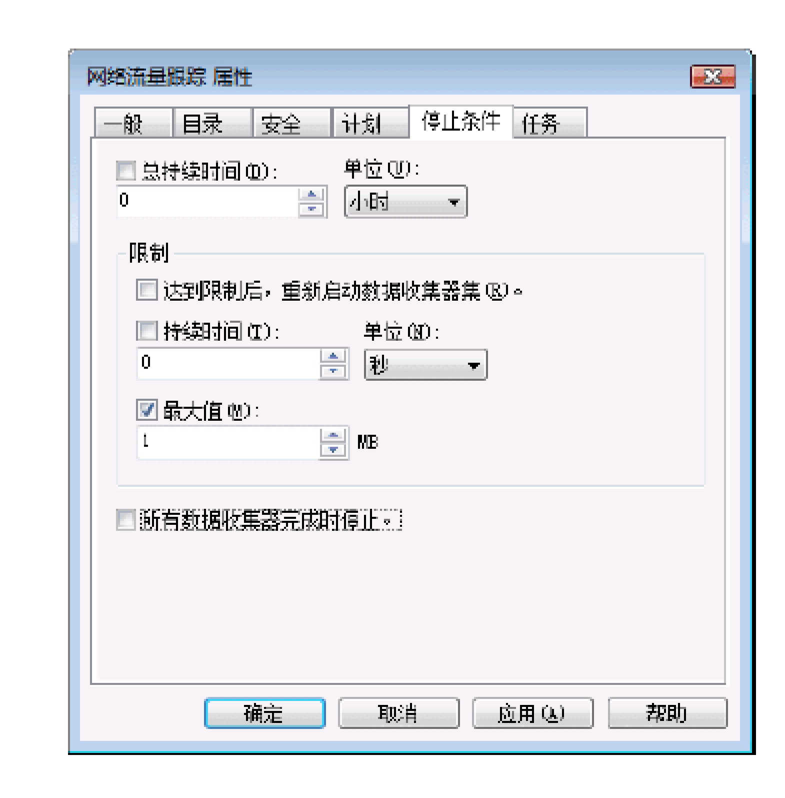


图 8-50　设置停止条件

8.3.6　可靠性监视器

可靠性监视器可以计算系统稳定性指数，该指数反映意外问题是否降低了系统的可靠性。稳定性指数的时间图会快速标识问题开始发生的日期。提供的系统稳定性报告提供了详细信息，以帮助解决可靠性降低的问题。通过逐个查看对故障系统(应用程序故障、操作系统崩溃或硬件故障)的更改(安装或删除应用程序，更新操作系统，或者添加或修改驱动程序)，可以形成一个解决问题的策略。

如图 8-51 所示，在该界面中，各项的含义如下。

- 红色叉号所在的位置表示 Windows Server 2008 系统在那一刻有错误操作存在。
- 黄色感叹号所在的位置表示 Windows Server 2008 系统在那一刻有安全隐患操作存在。
- 绿色字母 i 符号所在的位置表示 Windows Server 2008 系统在那一刻有操作成功的提示信息存在。
- 图表上面的黑色小方块表示 Windows Server 2008 系统每一天的事件采集点。每一个事件采集点包含的信息主要有五个方面，分别如下。
    - Windows 故障信息。
    - 硬件故障信息。
    - 应用程序故障信息。
    - 软件安装卸载信息。
    - 其他故障信息。

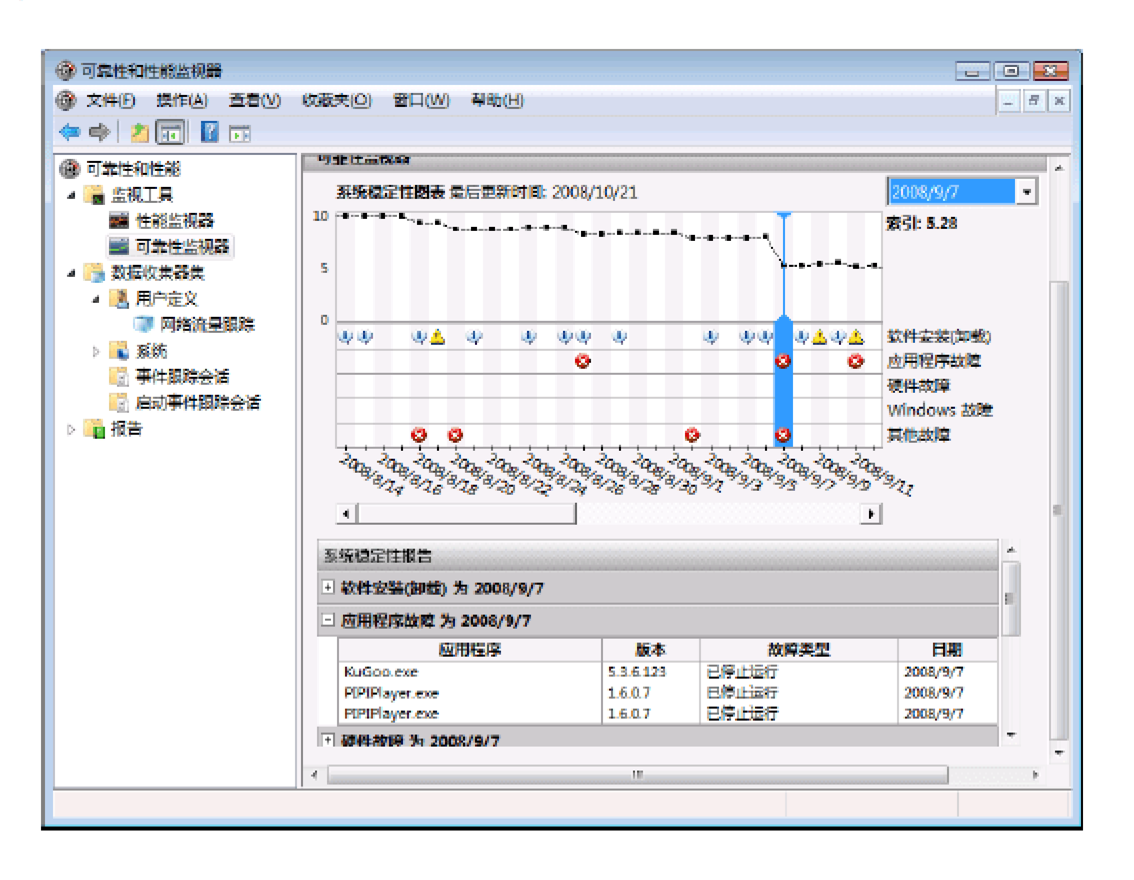


图 8-51　可靠性监视

Windows Server 2008 系统会自动对每一个事件采集点收集来的五方面信息进行综合评估，并对系统的运行稳定性进行量化评分，其中最稳定的系统状态，其可靠性的评估分为 10 分。从图 8-51 所示的界面中不难看出随着系统运行时间的推移，系统运行的可靠性也逐步下降。



提示：就笔者自己的计算机系统来看，2008 年 9 月 6 日之前的系统可靠性是最好的，不过从 9 月 6 日开始，系统运行可靠性开始下降，很明显，笔者自己的计算机系统最理想的系统还原点应该处于 9 月 6 日之前，也就是说当笔者的系统遇到意外需要还原时，我们必须将系统还原点设定在 9 月 6 日之前的某个时刻，这样一来系统的工作状态才能被恢复到最稳定、最健康的状态。

8.4 Windows 系统资源管理器

通过用于 Windows Server 2008 操作系统的 Windows 系统资源管理器，可以使用标准资源策略或自定义资源策略来管理服务器的处理器和内存的使用情况。通过管理资源，可以帮助确保均等地使用一台服务器提供的所有服务，或确保高优先级的应用程序、服务或用户始终可以使用你的资源。

仅当组合的处理器负荷大于 70% 时，Windows 系统资源管理器才会管理处理器资源。这意味着在处理器负荷较小时，不会主动限制每个使用者可以占用的资源。如果发生处理器资源的争用，资源分配策略可以根据你定义的管理配置文件，帮助实现最低的资源可用性。

8.4.1 Windows 系统资源管理器的功能

可以使用 Windows 系统资源管理器执行下列操作。

- 使用预配置的策略管理系统资源(处理器和内存)，或创建自定义策略，按进程、按用户或按 Internet 信息服务 (IIS) 应用程序池分配资源。
- 使用日历规则在不同时间应用不同的策略，而不必人工干预或重新配置。
- 自动选择基于服务器属性和事件(例如群集事件或条件)的资源策略，或基于已安装物理内存大小或处理器个数的更改的资源策略。
- 在本地或自定义 SQL 数据库中收集资源使用情况的数据。可以将多台服务器中的资源使用情况数据合并到一台运行 Windows 系统资源管理器的计算机上。

资源管理的作用

由于 Windows Server 2008 设计为向非操作系统任务提供尽可能多的资源，所以，运行单个角色的服务器通常不要求进行资源管理。但是，如果一台服务器上安装了多个应用程序和服务，这些应用程序和服务并不会察觉到进程的争用。不受管理的应用程序或服务通常将使用所有可用资源来完成任务。因此，使用 Windows 系统资源管理器等工具来管理多用途服务器上的系统资源是非常重要的。使用 Windows 系统资源管理器主要有两个好处。

- 由于通过动态管理的资源可以提高服务的可用性，所以，可以在一台服务器上运行更多的服务。
- 即使处于最大资源负荷期间，高优先级的用户或系统管理员仍可以访问系统。

8.4.2 Windows 系统资源管理器中的内存管理

可以在 Windows 系统资源管理器中创建资源分配，用于限制进程使用的工作集内存量或提交内存量。

内存限制按进程应用。例如，如果创建一个资源分配策略，将工作集限制指定为 10 MB，并将其应用于与 6 个正在运行的进程匹配的进程匹配条件，10 MB 的限制将分别应用于全部 6 个进程。

1. 工作集内存限制

可以为匹配进程的工作集设置上限。Windows 系统资源管理器禁止匹配进程的工作集超过在资源分配中定义的限制。如果达到限制，后续的内存分配不会失败，但是将替换工作集中的现有页面。这样可以避免后续的应用程序错误。

2. 提交内存的限制

可以为进程使用的提交内存设置上限。通常，如果进程使用的提交内存持续增大，则是由于进程中的内存泄漏所致。在为进程使用的提交内存量设置限制时，如果发生内存泄漏，可以人工干预。达到限制后，Windows 系统资源管理器可以将事件记入事件日志，终止进程，或重新启动进程。

Windows 系统资源管理器服务维护提交内存的限制。该服务监视匹配进程对提交内存的利用率。只要进程对提交内存的利用率超过该服务的限制，该服务还会强制执行用户定义的操作。

3. 其他考虑事项

不要使用 Windows 系统资源管理器中的内存限制来动态管理或修改自己的内存限制的应用程序或进程，这样可能会影响 Windows 系统资源管理器以及所管理的应用程序的正常运行。

最佳做法是，使用 CPU 目标来管理资源。有选择地将内存限制应用于出现内存耗尽问题的应用程序。如果过度地限制应用程序可以使用的内存，可能会延长应用程序完成任务的时间，并且可能会提高磁盘利用率。

8.4.3　安装 Windows 系统资源管理器

若要使用 Windows 系统资源管理器管理资源，必须安装 Windows 系统资源管理器功能，并且必须正在运行 Windows 系统资源管理器服务。



提示：安装 Windows 系统资源管理器功能，必须是本地 Administrators 组中的成员身份或等效身份。

安装 Windows 系统资源管理器功能操作如下。

① 选择“开始”→“管理工具”命令，然后选择“服务器管理器”命令。此时将启动 Microsoft 管理控制台。

② 在控制台窗格中，向下滚动到“功能摘要”选项。

③ 单击“添加功能”按钮。此时将启动添加功能向导。

④ 如图 8-52 所示，在功能列表中，选中“Windows 系统资源管理器”复选框，然后单击“下一步”按钮。

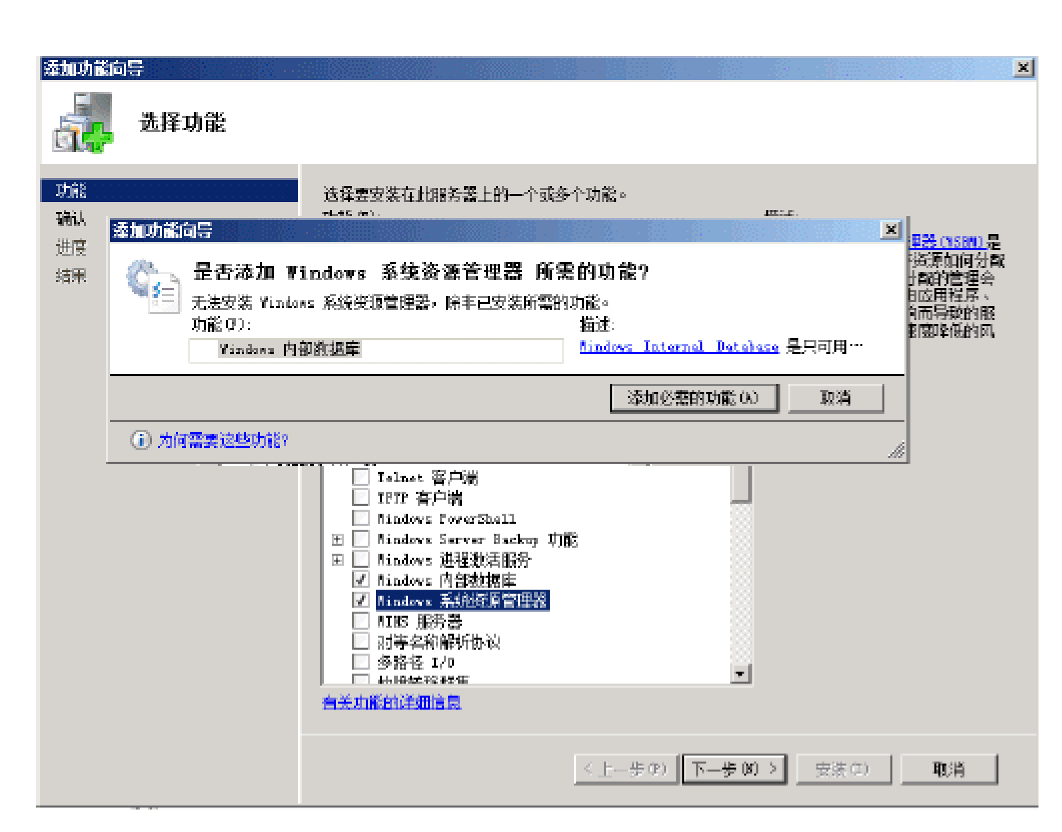


图 8-52　安装资源管理器

⑤ 按照向导中的步骤完成 Windows 系统资源管理器的安装。

8.4.4 Windows 系统资源管理器中的处理器管理

Windows 系统资源管理器通过调整进程优先级来管理处理器资源。这样，可以保证进程匹配条件定义的进程组可以获得最低可用 CPU 带宽百分比。除非总 CPU 利用率大于 70%，否则，不会强制进行资源管理。

还可以使用 Windows 系统资源管理器来定义处理器关联。这意味着匹配的进程可以与多处理器计算机上的一个处理器或一组处理器关联。



注意：永远不要管理核心操作系统进程，包括 Windows 系统资源管理器服务。此外，可以手动将进程添加到用户定义的排除列表中，以便不进行管理。排除的进程或非受管理进程组成员的进程必须共享在分配之后剩余的资源。

1. 处理器管理方法

Windows 系统资源管理器可以通过 CPU 百分比目标或处理器关联规则来管理处理器资源。



注意：如果应用程序具有管理 CPU 使用情况或处理器关联的功能，应使用其自带的资源管理功能并将其添加到用户定义的排除列表中。

2. CPU 百分比目标

分配处理器资源最简单的方法是为进程匹配条件定义的每个进程组分配一个 CPU 百分比目标。此目标是向进程组保证的最低可用 CPU 带宽百分比。



注意：可以分配的资源是核心操作系统进程或手动排除的进程未使用的资源。

由于 Windows 系统资源管理器保证最低可用 CPU 带宽，而不是限制 CPU 带宽的利用率，所以，受管理的进程组使用的实际 CPU 可能会超过最低分配。同样，未使用其最低分配的受管理进程组的多余容量将重新分配给需要更多资源的进程组。

3. 管理规则

在使用 CPU 约束创建资源分配策略时，还可以选择要应用的管理规则。这些管理规则类似于内置的资源分配策略，但是在将其应用于资源分配策略中的一个资源分配时，将在该资源分配的所有匹配进程之间分配已分配的 CPU。

管理规则包括如下内容。

- 标准(默认值)。Windows 系统资源管理器不会尝试控制在匹配的进程之间分配已分配的 CPU 的方式。选择此管理规则时，可以使用附加的进程匹配条件向匹配的进程二次分配资源。例如，一个匹配的进程可能会使用所有已分配的 CPU 带宽。Windows 系统资源管理器不会管理此带宽使用，所以，可能会影响其他进程。
- 每进程相等。可用的 CPU 带宽在匹配的进程之间平均分配。选择此管理规则时，不允许进行二

次分配。例如，如果两个匹配的进程使用已分配的 CPU 带宽的 100%，Windows 系统资源管理器将降低 CPU 利用率超过 50% 的进程的优先级。

- 每用户相等。每个用户运行的匹配进程组共享的可用 CPU 带宽相等。选择此管理规则时，不允许进行二次分配。例如，如果两个用户正在运行多个应用程序，这些应用程序使用已分配的 CPU 带宽的 100%，Windows 系统资源管理器将降低 CPU 利用率超过 50% 的用户所运行的进程的优先级。
- 每会话相等。在终端服务器上，每个终端服务会话中运行的匹配进程共享的可用 CPU 带宽相等。选择此管理规则时，不允许进行二次分配。例如，如果连接到终端服务器的两个用户使用已分配的 CPU 带宽的 100%，Windows 系统资源管理器将降低 CPU 利用率超过 50% 的终端服务器会话中运行的进程的优先级。
- 二次分配。CPU 百分比目标分配可以进一步分为二次分配。二次分配按父级资源分配所分配的资源的百分比计算所分配的资源。此二次分配匹配的进程匹配条件与父级资源分配不同。二次分配优先于默认的资源分配策略。
- 每进程相等(默认管理规则)。在一个进程组中的进程之间管理资源的默认策略是内置策略 Equal_Per_Process。通过此策略可以实现如下功能。
  - 可用的 CPU 带宽在进程匹配条件所确定的进程之间平均分配。
  - 默认情况下启用超越进程保护。
  - 如果启动 Windows 系统资源管理器而不进行其他配置，则将此策略应用于受管理的服务器上运行的所有可管理进程。
  - 此默认策略可以通过编辑 Windows 系统资源管理器属性进行更改。应启用“当前资源分配策略”(如果禁用了日历)或禁用“日历默认策略”(如果启用了日历)。

4. 处理器关联

除了指定 CPU 目标百分比之外，匹配的进程还可以与多处理器系统上的特定处理器关联。此方法可以在少量进程匹配条件之间分配服务器的资源，但是，在对大量进程匹配条件使用处理器关联时，应谨慎操作。Windows 系统资源管理器在计算具有关联的进程的可用资源时，将只考虑一个处理器的状态。所以，如果系统遇到较高负荷，可能会过度分配处理器资源。

有时，可用的 CPU 带宽可能会低于预期。这样，将减少分配给匹配进程的 CPU 带宽，可能会使这些进程的响应速度低于预期。如果符合下列条件，则可能会发生这种情况。

- 进程组关联的处理器数过少。
- 没有关联的进程使用另一个进程组约束到的处理器。
- 进程匹配条件无法检查在具有关联的进程之间是否存在分配冲突。



注意：对于 SQL Server 多实例管理，不建议通过 Windows 系统资源管理器管理 CPU 关联，而应使用 SQL Server 的处理器关联设置。

8.4.5　内置的资源管理策略

可以通过选择要使用的策略类型来启用内置的资源管理策略。无须执行其他配置。

- 每进程相等。使用 Equal_Per_Process 资源分配策略管理系统时，将同等对待每个正在运行的进程。例如，如果运行 10 个进程的服务器达到 70% 的处理器利用率，当这些进程处于争用状态时，Windows 系统资源管理器就将限制每个进程最多占用处理器资源的 10%。注意，低利用率进程未使用的资源将分配给其他进程。
- 每用户相等。使用 Equal_Per_User 资源分配策略管理系统时，根据运行进程的用户账户对进程进行分组，并同等对待每个进程组。例如，如果 4 个用户正在服务器上运行进程，将为每个用户分配系统资源的 25% 来完成这些进程。分配给运行一个应用程序的用户的资源与分配给运行多个应用程序的用户相同。此策略对于应用程序服务器尤其有用。
- 每会话相等。使用 Equal_Per_Session 资源分配策略管理系统时，为连接到系统的每个会话分配相等的资源。此策略适用于终端服务器。
- 每 IIS 应用程序池相等。使用 Equal_Per_IISAppPool 资源分配策略管理系统时，将同等对待每个正在运行的 IIS 应用程序池，不在 IIS 应用程序池中的应用程序只能使用 IIS 应用程序池未使用的资源。

示例：指定服务器使用内置的资源管理策略。

Web 服务器上有多个 Web 站点，每个 Web 站点使用独立的应用程序池。为避免某一个 Web 站点的应用程序池过多地使用 Web 服务器资源而影响其他 Web 站点的性能，需要指定 Windows 资源管理器中默认的 Equal_Per_IISAppPool 策略为管理策略。

① 选择“开始”→“程序”→“管理工具”→“Windows 系统资源管理器”命令。

② 可以看到系统内置的资源管理策略，当前生效的策略是 Equal_Per_Process。

③ 如图 8-53 所示，右击 Equal_Per_IISAppPool 选项，在弹出的快捷菜单中选择“设置为管理策略”命令，在“警告”对话框中，单击“确定”按钮。日历被禁用。

④ 图 8-54 所示，可以看到 Equal_Per_IISAppPool 策略生效。日历被禁用。


注意：系统资源分配策略可以有多个，但在某一时刻只能有一个生效。

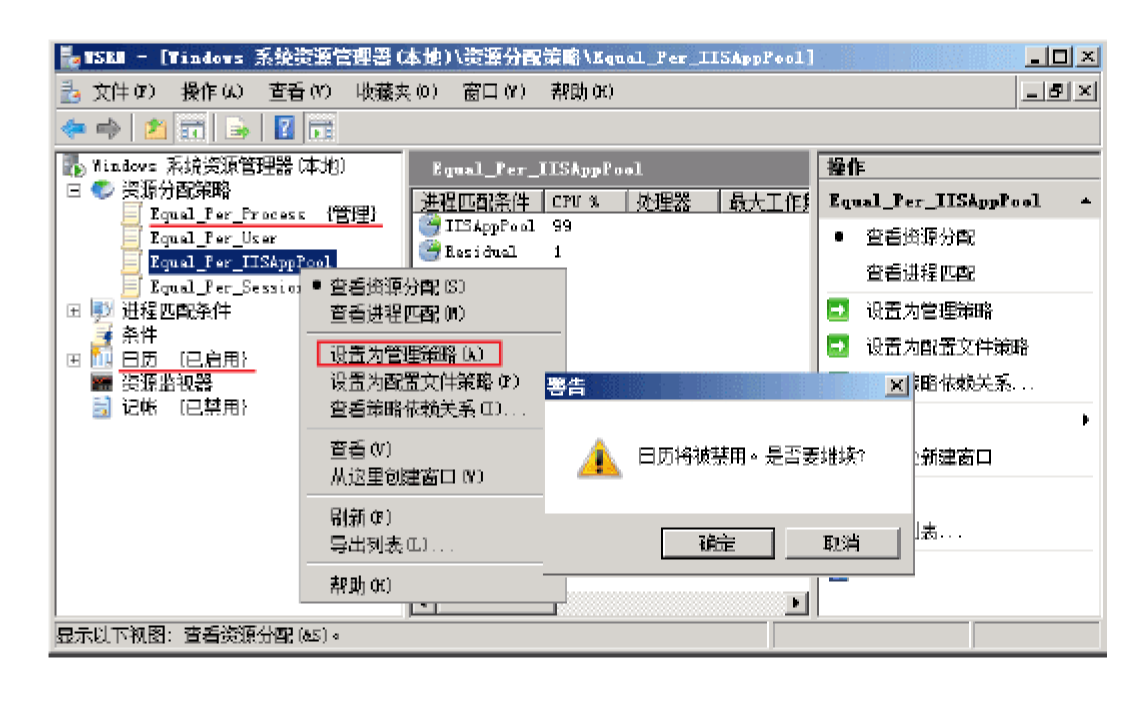


图 8-53　应用默认策略

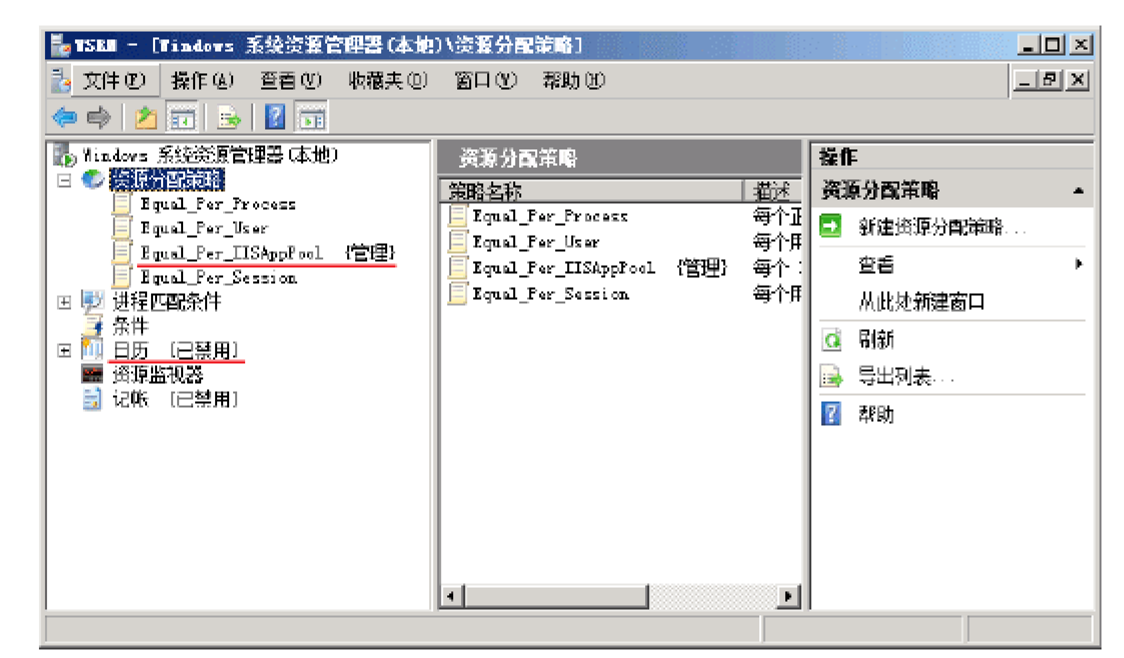


图 8-54　生效的策略

8.4.6　自定义资源管理

可以使用自定义资源管理方法来确定资源用户，并根据自己的条件为这些用户分配资源。

- 进程匹配条件。使你可以选择要受资源分配策略规则管理的服务或应用程序。可以通过文件名或命令进行选择，也可以指定用户或组。例如，可以创建一个进程匹配条件，对 Administrator 用户运行的应用程序 iexplore.exe 实施管理。
- 资源分配策略。为你创建的进程匹配条件所指定的进程分配处理器资源和内存资源。
- 排除列表。使应用程序、服务、用户或组不受 Windows 系统资源管理器管理。



注意：也可以在资源分配策略中使用命令行路径匹配，使应用程序不受该策略的管理。

- 计划。使用日历界面控制一次性事件或对资源分配的定期更改。不同的资源分配策略可以在每天的不同时间、每周的不同天或根据其他计划方法处于活动状态。
- 条件策略的应用。自动切换资源分配策略，以响应特定系统事件(例如，安装新内存或其他处理器，启动或停止节点，或更改群集中的某个资源组的可用性)。

示例 1：利用日历安排系统资源管理策略。

可以利用日历安排 Windows 系统资源管理策略。

比如每天 8:00 到 12:00 的时间段使用 Equal_Per_IISAppPool 策略，14:00 到 16:00 的时间段使用 Equal_Per_Process 策略。

① 选择“开始”→“程序”→“管理工具”→“Windows 系统资源管理器”命令。

② 右击“日历”选项，在弹出的快捷菜单中选择“启用”命令。

③ 右击如图 8-55 所示的位置，在弹出的快捷菜单中选择“新建定期事件”命令。

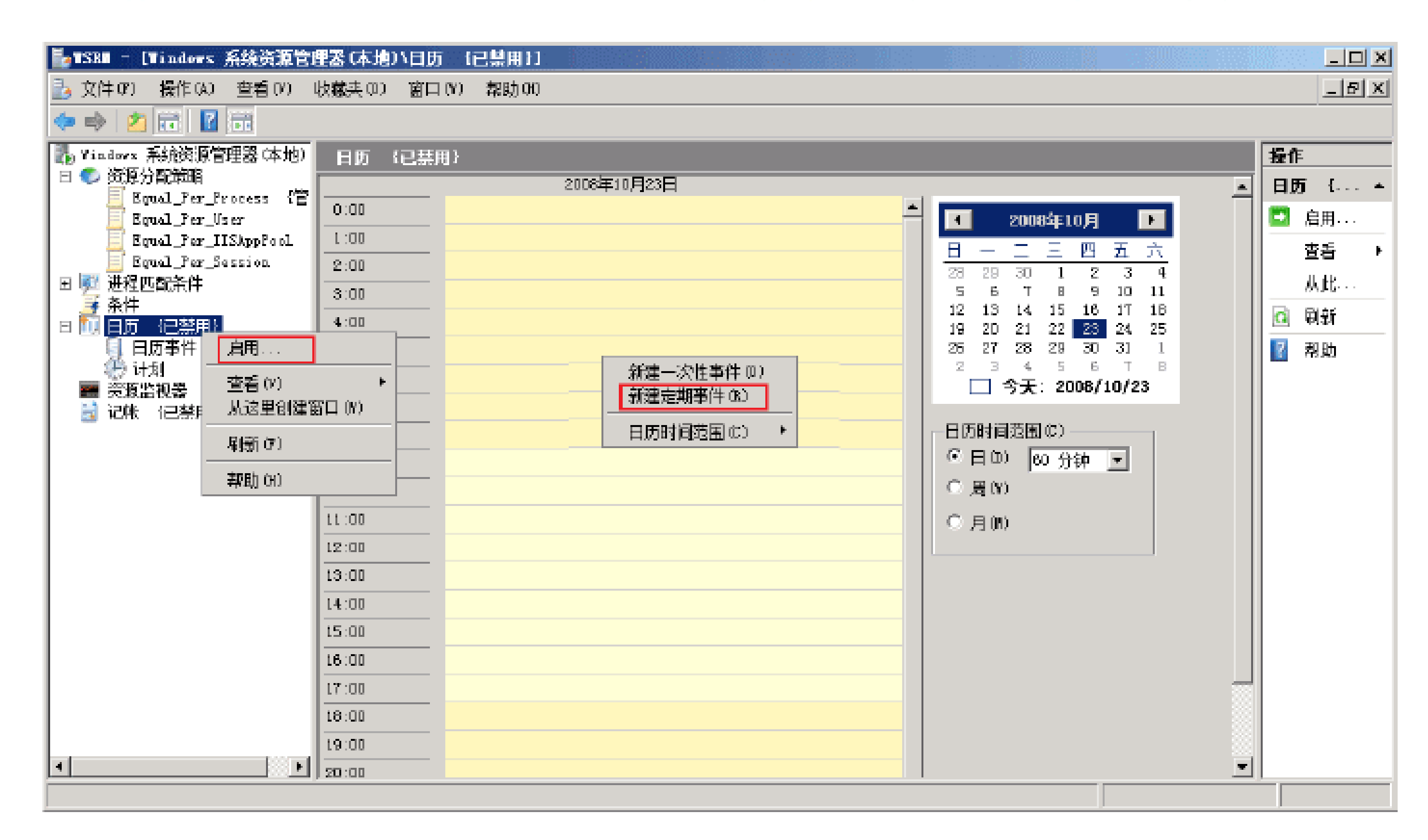


图 8-55 创建定期事件

④ 如图 8-56 所示，输入事件名 Equal_Per_IISAppPool，设置开始时间和结束时间，策略名称选择 Equal_Per_IISAppPool，单击“确定”按钮。

⑤ 如图 8-57 所示，再新建定期事件，事件名输入 Equal_Per_Process，策略名称选择 Equal_Per_Process。

⑥ 如图 8-58 所示，可以看到由日历安排系统使用的系统资源配置策略。

⑦ 更改系统时间，会发现在不同的时间段，系统将会使用不同的策略。

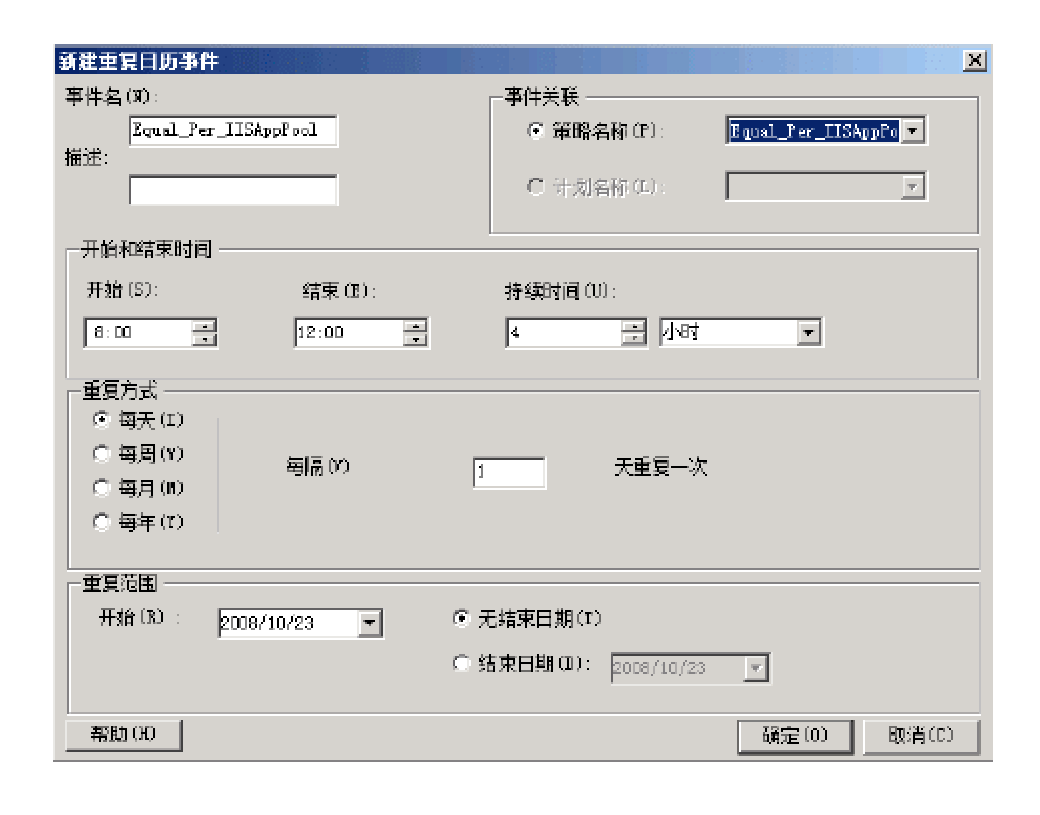


图 8-56　设置开始时间和结束时间

图 8-57　新建定期事件

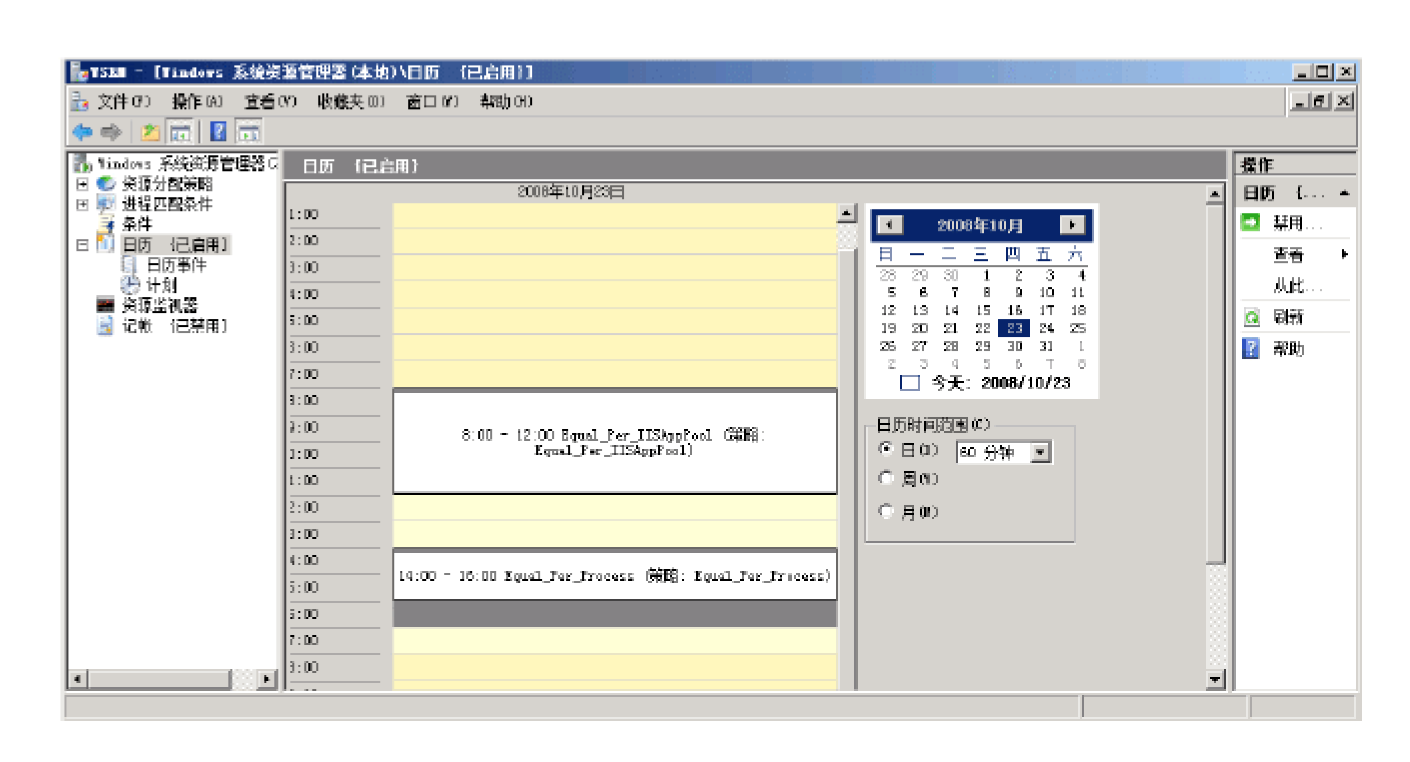


图 8-58　日历安排策略

示例 2：创建自定义的资源分配策略。

指定 Administrator 使用记事本程序的系统资源分配策略。

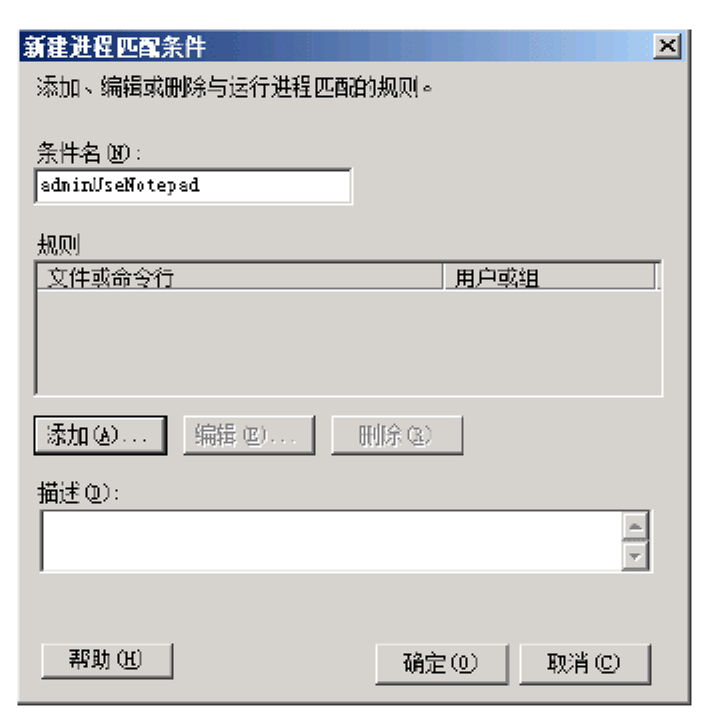
① 如图 8-59 所示，单击“新建进程匹配条件”选项。



图 8-59　新建进程匹配条件

② 如图 8-60 所示，在“新建进程匹配条件”对话框中，输入条件名 adminUseNotepad，单击“添加”按钮。

③ 如图 8-61 所示，在“添加规则”对话框中，从下拉列表框中选择“应用程序”，单击“选择”按钮。



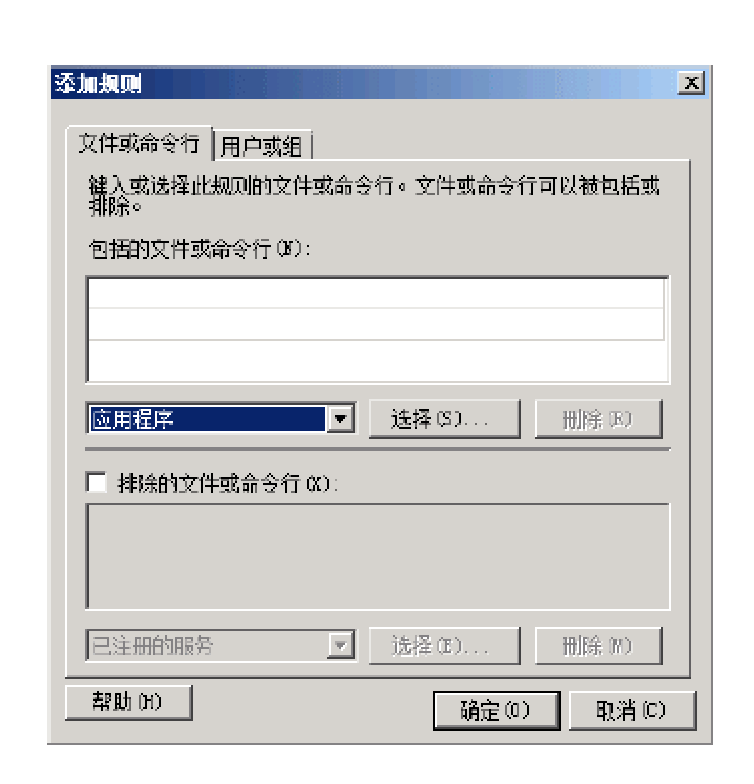
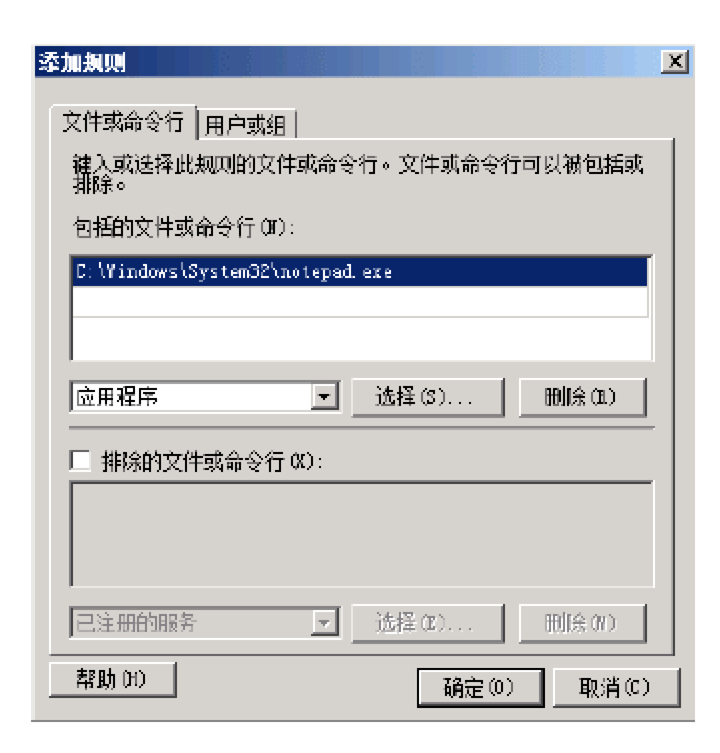



图 8-60　输入条件名

图 8-61　选择应用程序

④ 如图 8-62 所示，在打开的对话框中，输入%SystemRoot%\system32\notepad.exe，单击“确定”按钮。

⑤ 如图 8-63 所示，切换到“用户或组”选项卡，单击“添加”按钮，输入 administrator，单击“确定”按钮。



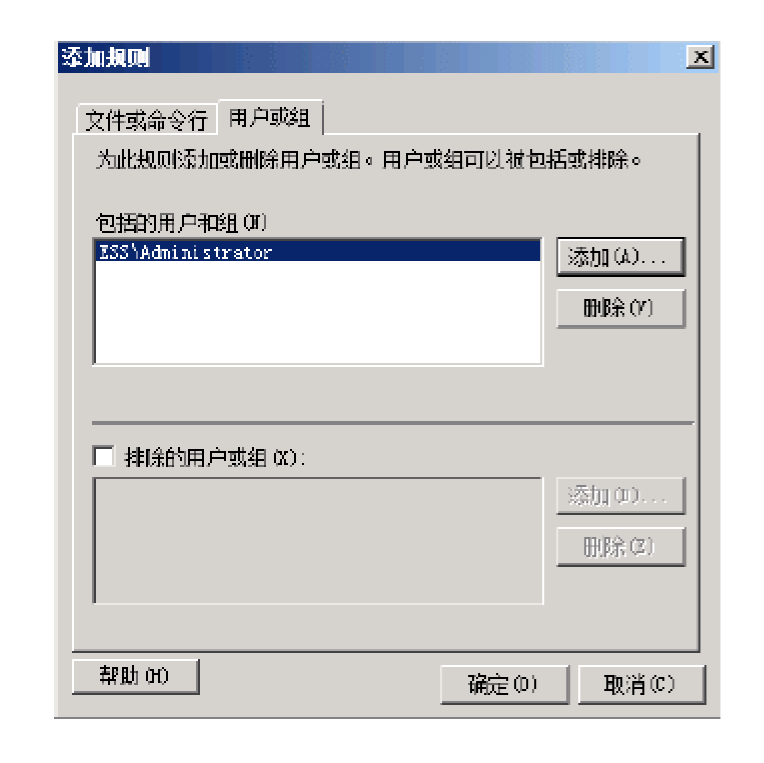


图 8-62　选择记事本程序

图 8-63　添加用户

⑥ 如图 8-64 所示，单击“资源分配策略”选项，单击“新建资源分配策略”按钮。

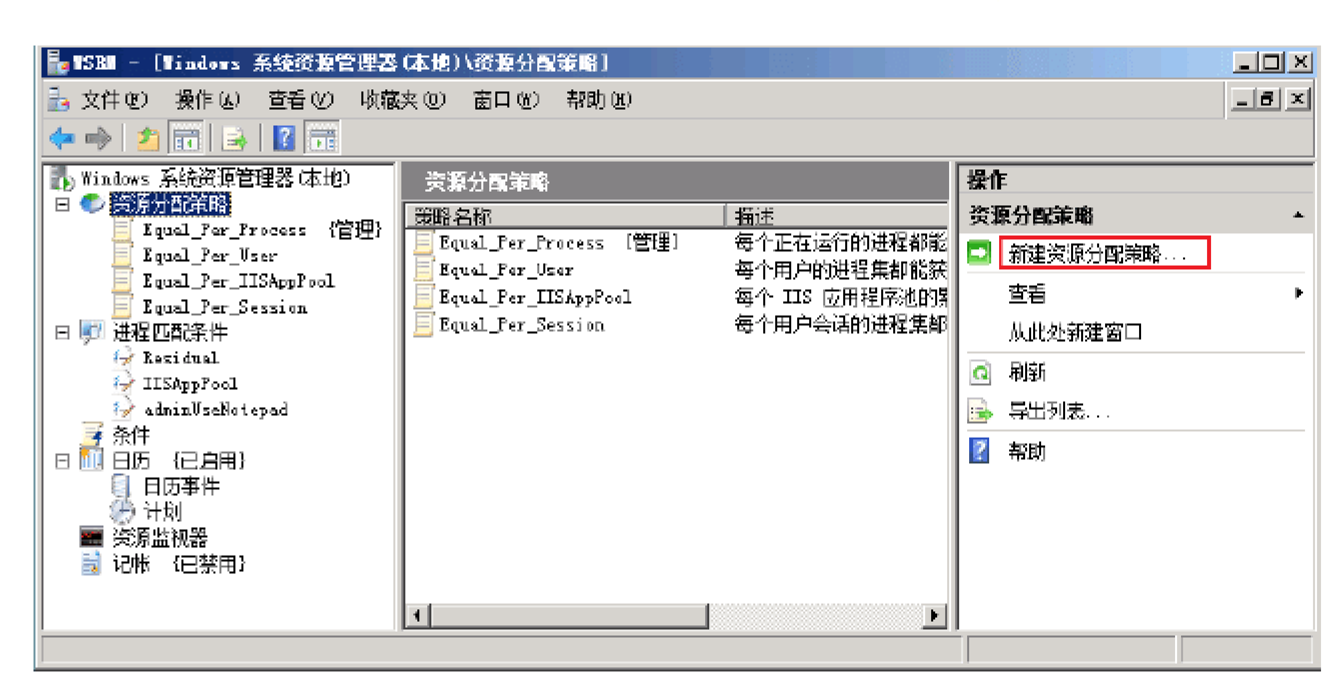


图 8-64　创建资源分配策略

⑦ 如图 8-65 所示，在“新建资源分配策略”对话框中，输入策略名称“限制管理员使用记事本”，单击“添加”按钮。

⑧ 如图 8-66 所示，在“添加或编辑资源分配”对话框中，进程匹配条件选中 adminUseNotepad，为此资源分配的处理器的百分比为 2。切换到“内存”选项卡。

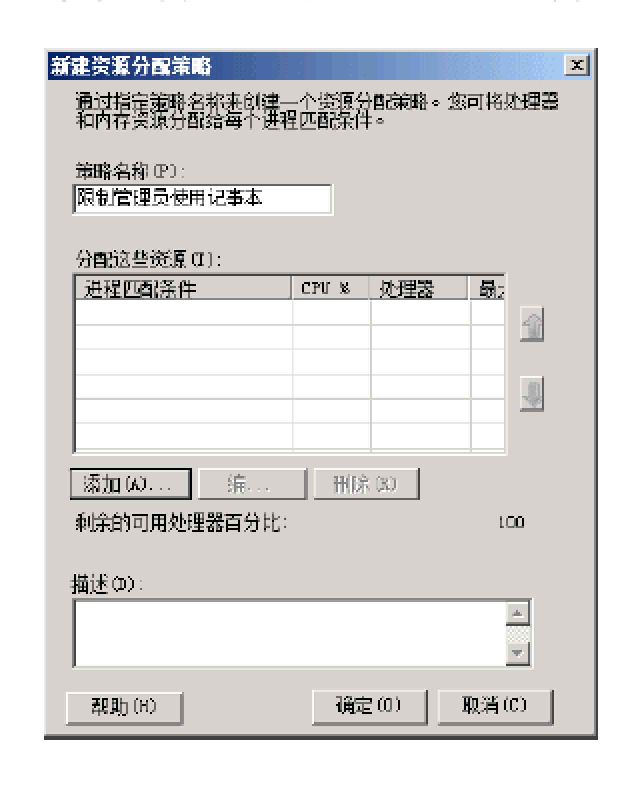


图 8-65 输入策略名称

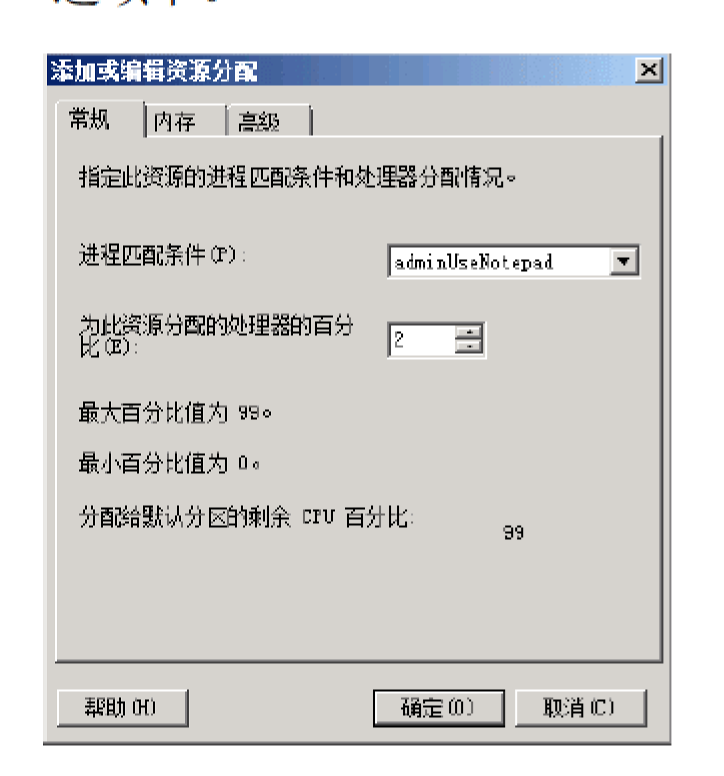


图 8-66 选择进程匹配条件

⑨ 如图 8-67 所示，限定最大内存 1 MB。如果超过了内存，选中“停止此应用程序”选项，单击“确定”按钮。

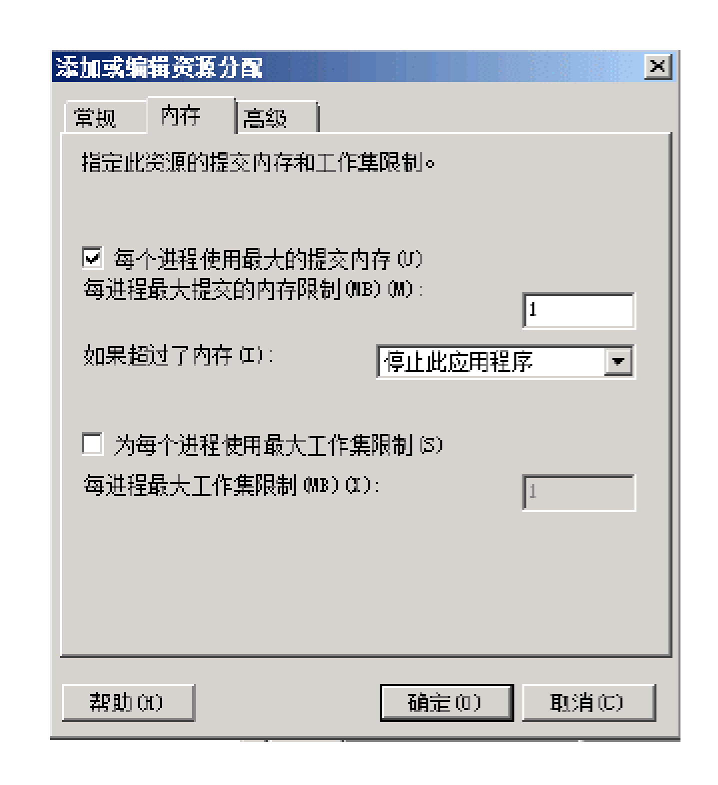


图 8-67 选择内存最大限制

⑩ 如图 8-68 所示，右击刚才创建的策略，在弹出的快捷菜单中选择“设置为管理策略”命令，这样就禁止了日历中的安排。



图 8-68 指定为管理策略

⑪ 打开记事本，你会发现，只要记事本程序占用的内存大于 1 MB，就会立即关闭记事本。

第 9 章　Windows Server 2008 安全策略

安全策略是影响计算机安全性的安全设置的组合。可以利用本地安全策略来编辑本地计算机上的账户策略和本地策略。

利用安全性策略，可以强化公司网络的安全性。这些安全性策略定义了一个公司对于正确使用计算机的期望值，也确定了特殊的过程，用于防止发生安全性事故和对已经发生的安全性事故做出响应。因此，由网络管理员保护工作站上桌面和服务的安全性是非常重要的。通过应用安全性策略，可以防止用户破坏计算机配置，并且可以保护网络中的敏感区域。

通过配置本地安全策略，可以加固服务器安全。从以下几个方面配置服务器安全：账户策略、审核策略、用户权限分配、安全选项及软件限制策略。

高级 Windows 防火墙能够控制进入操作系统的流量，也能够控制出去的流量，还能够配置服务器之间进行加密的通信。

关键词

- 配置系统的账户策略
- 启用审核策略
- 配置用户权限分配
- 配置安全选项
- 配置高级的 Windows 防火墙
- 配置软件限制策略
- 使用本地组策略配置系统安全

9.1 配置工作组计算机系统安全

任务描述

- 配置工作组中计算机的系统安全。
- 配置域中计算机的系统安全。

实战环境

- DCServer 是 Ess.com 域的域控制器，操作系统是 Windows Server 2008 企业版。
- Sales 是该域的计算机，操作系统是 Vista。
- WorkgroupServer 是工作组中的计算机，操作系统是 Windows Server 2008 企业版。

实战目标

学会配置工作组中计算机的系统安全。

9.2 账户策略的设置

9.2.1 设置密码策略

1. 为工作组中的计算机设置密码策略

① 以管理员的身份登录 WorkgroupServer 计算机。

② 选择“开始”→“程序”→“管理工具”→“本地安全策略”命令。

③ 选择“帐户策略”下的“密码策略”选项，可以看到如图 9-1 所示的几项设置。

④ 按照图 9-2 所示，设置安全策略。

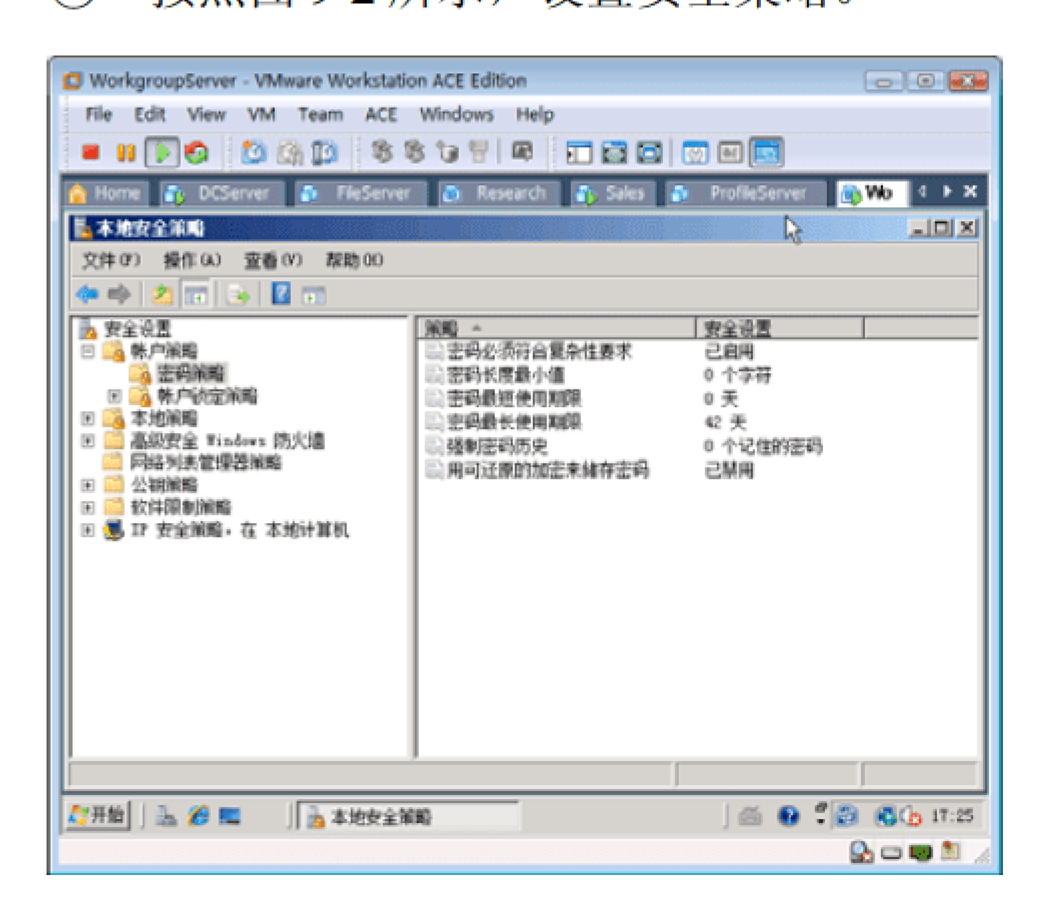


图 9-1 密码策略

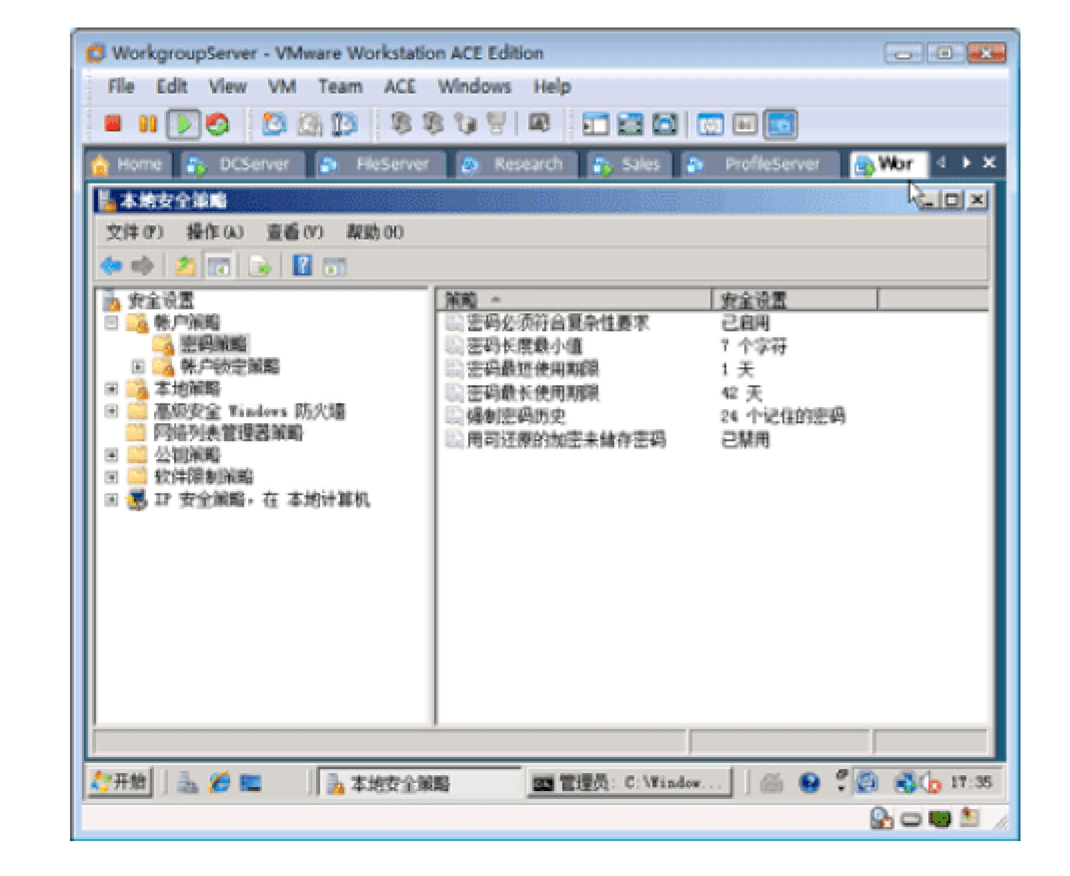


图 9-2 设置安全策略

⑤ 如图 9-3 所示，进入命令行，以下是创建用户时密码不满足策略的情况。

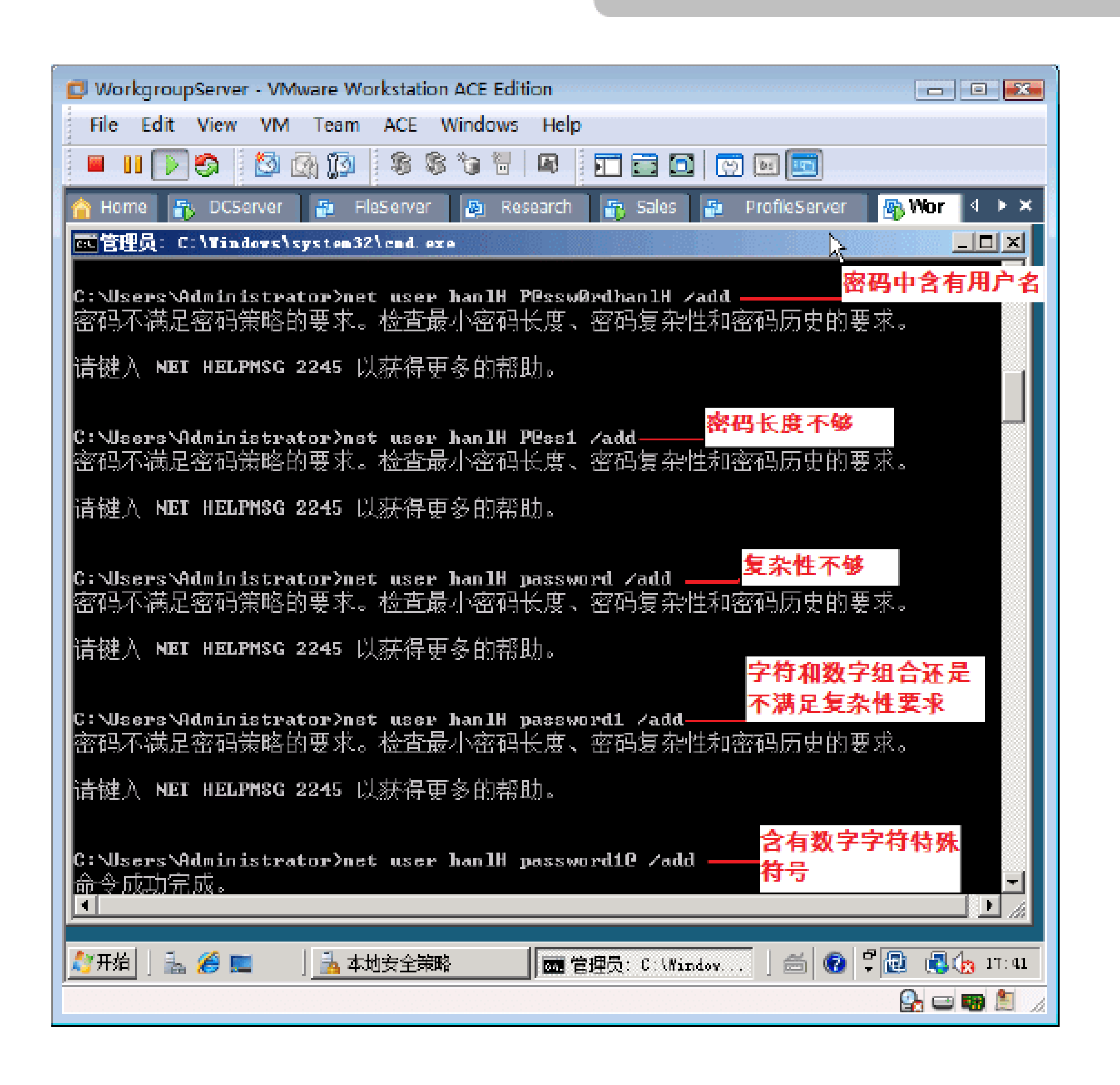


图 9-3　密码要求

2. 密码必须符合复杂性要求

此安全设置确定密码是否必须符合复杂性要求。

如果启用此策略，密码必须符合下列最低要求。

- 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。
- 至少有 6 个字符长。
- 包含以下四类字符中的三类字符。
  - 英文大写字母(A～Z)。
  - 英文小写字母(a～z)。
  - 10 个基本数字(0～9)。
  - 非字母字符(例如：!、$、#、%)。

3. 最短密码长度

此安全设置确定用户账户密码包含的最少字符数。可以将值设置为介于 1～14 字符之间，或者将字符数设置为 0，以确定不需要密码。

4. 密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位)。可以设置一个介于 1～998 天之间的值，或者将天数设置为 0，允许立即更改密码。

密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0，指明密码永不过期。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0～998 之间的任何值。

如果希望“强制密码历史”有效，则需要将密码最短使用期限设置为大于 0 的值。如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改管理员定义的密码。如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史”设置为 1。

5. 密码最长使用期限

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 1～999 之间)后到期，或者将天数设置为 0，指定密码永不过期。如果密码最长使用期限介于 1～999 天之间，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0～998 天之间的任何值。



注意：默认值为 42。安全最佳操作是将密码设置为 30～90 天后过期，具体取决于用户的环境。这样，攻击者用来破解用户密码以及访问网络资源的时间将受到限制。

6. 强制密码历史

此安全设置确定用户更改过多少次密码后才能使用以前的旧密码。该值必须介于 0～24 个密码之间。

此策略使管理员能够通过确保旧密码不被连续重新使用增强安全性。

若要维护密码历史的有效性，还要同时启用密码最短使用期限安全策略设置，不允许在密码更改之后立即再次更改密码。

7. 用可还原的加密来储存密码

使用此安全设置确定操作系统是否使用可还原的加密来储存密码。

此策略为某些应用程序提供支持，这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密储存密码与存储纯文本密码在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。

通过远程访问或 Internet 身份验证服务(IAS)使用质询握手身份验证协议(CHAP)验证时需要设置此策略。在 Internet 信息服务(IIS)中使用摘要式身份验证时也需要设置此策略。

默认值：禁用。

9.2.2 设置账户锁定策略

防止其他人无数次猜计算机上的用户账户密码，可以设置账户锁定阈值，如图 9-4 所示。

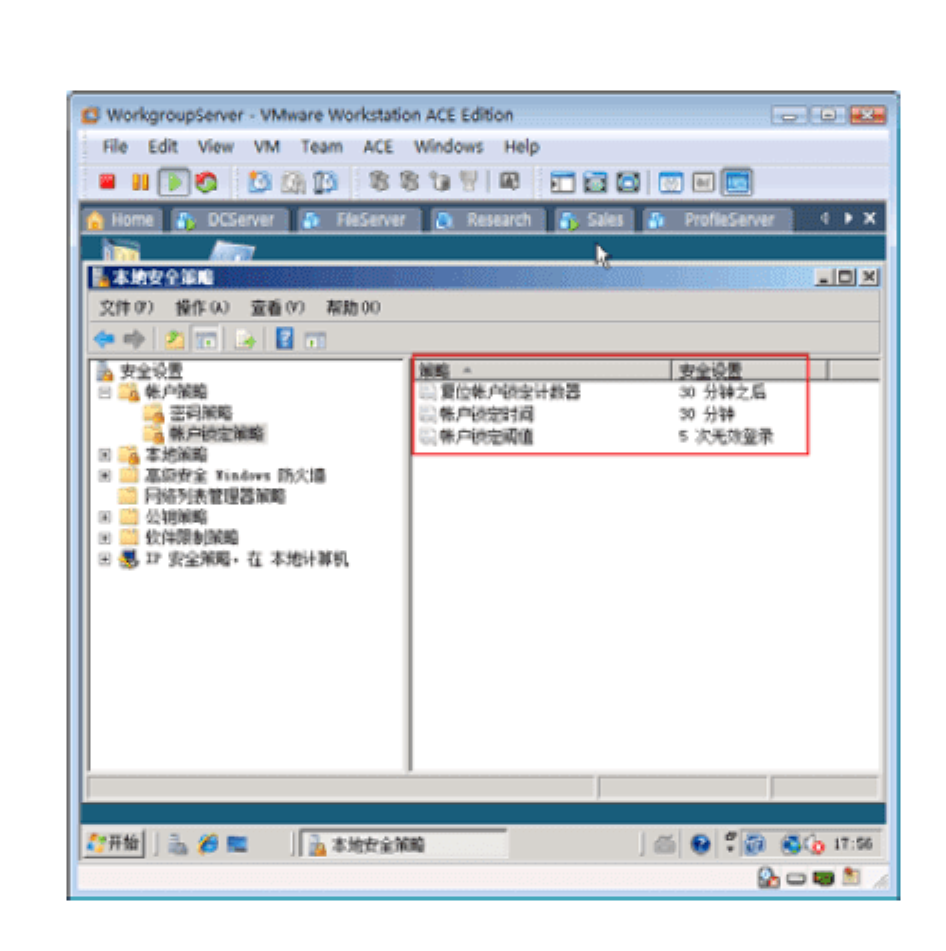


图 9-4 账户锁定策略

1. 账户锁定阈值

此安全设置确定导致用户账户被锁定的登录尝试失败的次数。在管理员重置锁定账户或账户锁定时间期满之前，无法使用该锁定账户。可以将登录尝试失败次数设置为介于 0～999 之间的值。如果将值设置为 0，则永远不会锁定账户。

在使用 Ctrl+Alt+Del 组合键或密码保护的屏幕保护程序锁定的工作站或成员服务器上的密码尝试失败将记作登录尝试失败。

2. 账户锁定时间

此安全设置确定锁定账户在自动解锁之前保持锁定的分钟数。可用范围从 0～99 999 min。如果将账户锁定时间设置为 0，账户将一直被锁定直到管理员明确解除对它的锁定。

如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间。

默认值：无。因为只有在指定了账户锁定阈值时，此策略设置才有意义。

3. 在此后复位账户锁定计数器

此安全设置确定在某次登录尝试失败之后将登录尝试失败计数器重置为 0 次错误登录尝试之前需要的时间。可用范围是 1～99 999 min。

如果定义了账户锁定阈值，此重置时间必须小于或等于账户锁定时间。

默认值：无。因为只有在指定了账户锁定阈值时，此策略设置才有意义。

4. 示例

如图 9-5 所示，切换用户，使用 hanlg 账户输入 5 次错误密码你会看到“引用的帐户当前已经锁定，且可能无法登录”的提示。

如图 9-6 所示，切换到管理员登录，打开服务器管理器，双击 hanlg 用户账号，可看到账户已经被锁定。

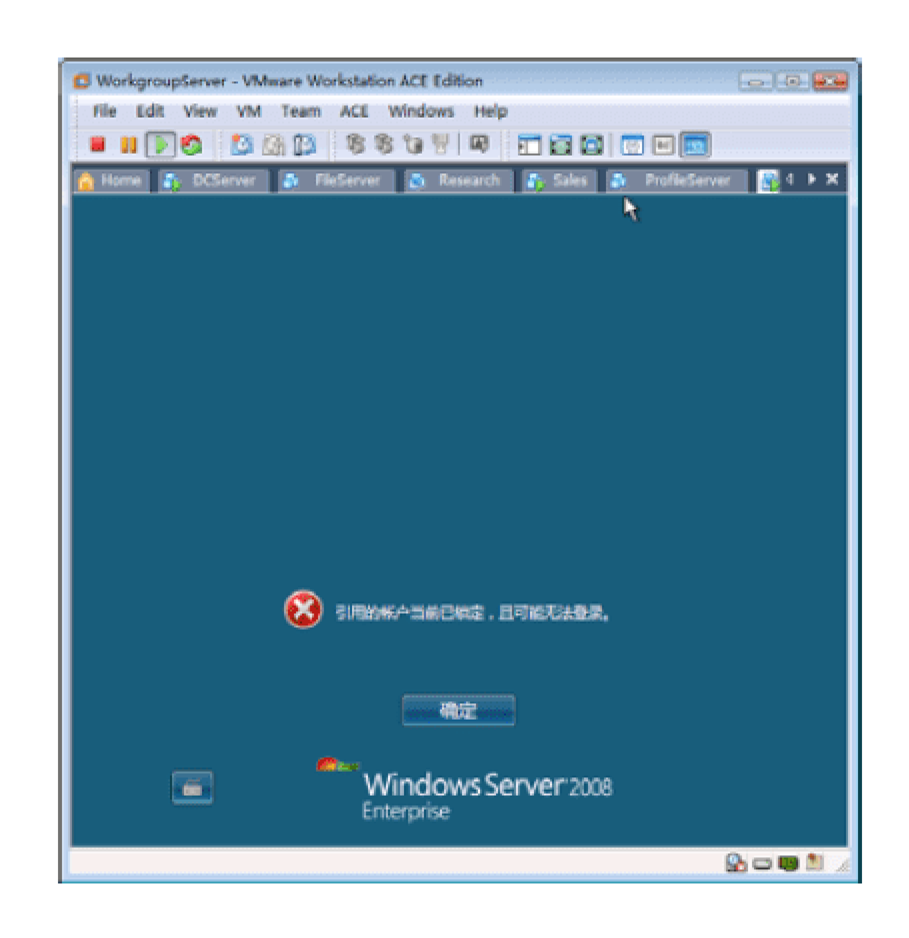


图 9-5　登录失败

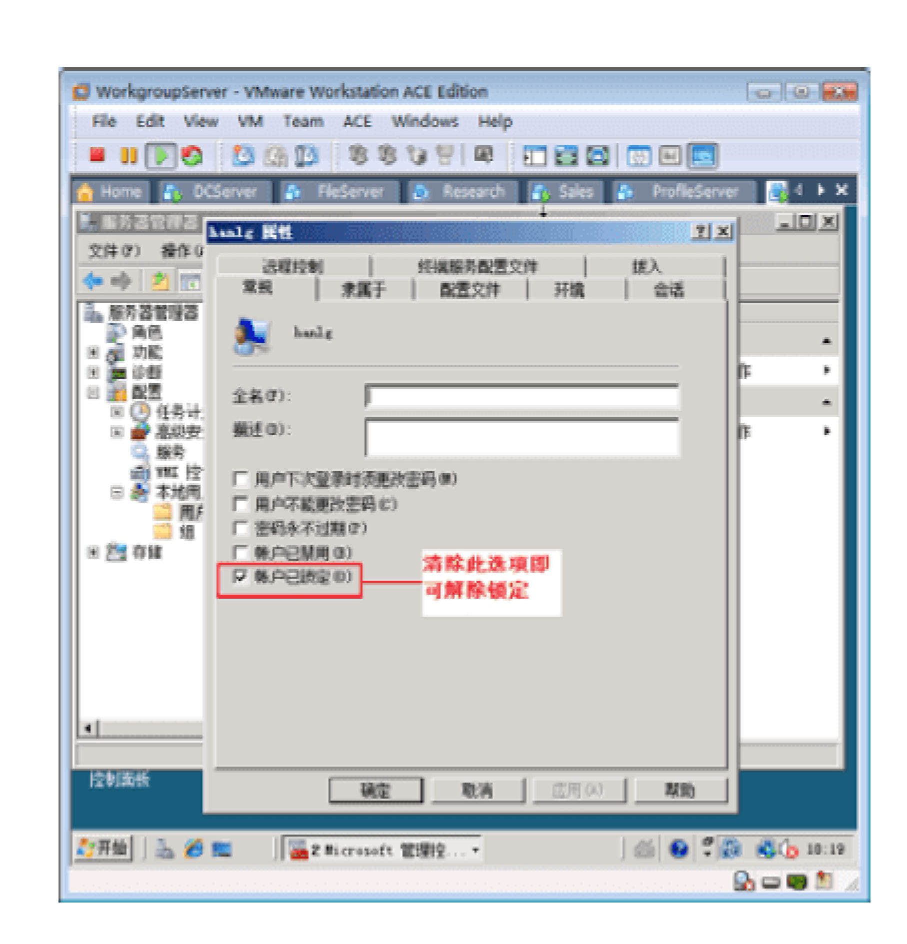


图 9-6　账户被锁定

9.3　设置审核策略

9.3.1　审核策略简介

本节介绍如何设置应用于审核的各种设置，并提供了由几个常见任务创建的审核事件示例。每当用户执行了指定的某些操作，审核日志就会记录一个审核项。可以审核操作中的成功尝试和失败尝试。

安全审核对于任何企业系统来说都极其重要，因为只能使用审核日志来说明是否发生了违反安全的

事件。如果通过其他某种方式检测到入侵，正确的审核设置所生成的审核日志将包含此次入侵的重要信息。

1. 简介

通常，失败日志比成功日志更有意义，因为失败通常说明有错误发生。例如，如果用户成功登录到系统，一般认为这是正常的。然而，如果用户多次尝试都未能成功登录到系统，则说明可能有人正试图使用他人的用户 ID 侵入系统。事件日志记录了系统上发生的事件。安全日志记录了审核事件。组策略的“事件日志”容器用于定义与应用程序、安全性和系统事件日志相关的属性，例如日志大小的最大值、每个日志的访问权限以及保留设置和方法。

2. 审核设置

所有审核设置的漏洞、对策和潜在影响都一样，因此这些内容仅在以下段落中详细讲述一次。然后在这些段落之后简要说明了每个设置。

审核设置的选项如下。

- 成功。
- 失败。
- 无审核。

3. 漏洞

如果未配置任何审核设置，将很难甚至不可能确定出现安全事件期间发生的情况。不过，如果因为配置了审核而导致有太多的授权活动生成事件，则安全事件日志将被无用的数据填满。为大量对象配置审核也会对整个系统的性能产生影响。

4. 对策

组织内的所有计算机都应启用适当的审核策略。这样合法用户可以对其操作负责，而未经授权的行为可以被检测和跟踪。

5. 潜在影响

如果在组织内的计算机上没有配置审核，或者将审核设置得太低，将缺少足够的甚至根本没有可用的证据，可在发生安全事件后用于网络辩论分析；而另一方面，如果启用过多的审核，安全日志中将填满毫无意义的审核项。

9.3.2 审核设置

1. 审核账户登录事件

“审核账户登录事件”设置用于确定是否对用户在另一台计算机上登录或注销的每个实例进行审核，该计算机记录了审核事件，并用来验证账户。如果定义了该策略设置，则可指定是否审核成功、失败或根本不审核此事件类型。成功审核会在账户登录尝试成功时生成一个审核项，该审核项的信息对于记账以及事件发生后的辩论十分有用，可用来确定哪个人成功登录到哪台计算机。失败审核会在账户登录尝试失败时生成一个审核项，该审核项对于入侵检测十分有用；但此设置可能会导致拒绝服务 (DDoS) 状态，因为攻击者可以生成数百万次登录失败，并将安全事件日志填满。

如果在域控制器上启用了账户登录事件的成功审核，则对于没有通过域控制器验证的每个用户，都会

为其记录一个审核项，即使该用户实际上只是登录到加入该域的一个工作站上。

2. 审核账户管理

“审核账户管理”设置用于确定是否对计算机中的每个账户管理事件进行审核。

账户管理事件的示例包括以下内容。

- 创建、修改或删除用户账户或组。
- 重命名、禁用或启用用户账户。
- 设置或修改密码。

如果定义了此策略设置，则可指定是否审核成功、审核失败或根本不审核此事件类型。成功审核会在任何账户管理事件成功时生成一个审核项，并且应在企业中的所有计算机中启用这些成功审核。在响应安全事件时，组织可以对创建、更改或删除账户的人员进行跟踪，这一点非常重要。失败审核会在任何账户管理事件失败时生成一个审核项。

3. 审核目录服务访问

“审核目录服务访问”设置用于确定是否对用户访问 Microsoft Active Directory 对象的事件进行审核，该对象指定了自身的系统访问控制列表(SACL)。SACL 是用户和组的列表。对象上针对这些用户或组的操作将在基于 Windows 2000 的网络中进行审核。

如果定义了此策略设置，则可指定是否审核成功、审核失败或根本不审核此事件类型。成功审核会在用户成功访问指定了 SACL 的 Active Directory 对象时生成一个审核项。失败审核会在用户试图访问指定了 SACL 的 Active Directory 对象失败时生成一个审核项。启用“审核目录服务访问”并在目录对象上配置 SACL，可以在域控制器的安全日志中生成大量审核项，因此仅在确实要使用所创建的信息时才应启用这些设置。

4. 审核登录事件

“审核登录事件”设置用于确定是否对用户在记录审核事件的计算机上登录、注销或建立网络连接的每个实例进行审核。如果正在域控制器上记录成功的账户登录审核事件，工作站登录尝试将不生成登录审核。只有域控制器自身的交互式登录和网络登录尝试才生成登录事件。总而言之，账户登录事件是在账户所在的位置生成的，而登录事件是在登录尝试发生的位置生成的。

如果定义了此策略设置，则可指定是否审核成功、审核失败或根本不审核此事件类型。成功审核会在登录尝试成功时生成一个审核项。该审核项的信息对于记账以及事件发生后的辩论十分有用，可用来确定哪个人成功登录到哪台计算机。失败审核会在登录尝试失败时生成一个审核项，该审核项对于入侵检测十分有用，但此设置可能会导致遭受 DDoS 攻击，因为攻击者可以生成数百万次登录失败，并将安全事件日志填满。

5. 审核对象访问

此安全设置确定是否审核用户访问指定了它自己的系统访问控制列表(SACL)的对象(例如文件、文件夹、注册表项及打印机等)的事件。

如果定义了此策略设置，可以指定是否审核成功、审核失败或者根本不审核该事件类型。成功审核在用户成功访问指定了相应 SACL 的对象时生成审核项。失败审核在用户尝试访问指定了 SACL 的对象失败时生成审核项。

注意：使用文件系统对象“属性”对话框中的“安全”选项卡，可以在该对象上设置 SACL。

9.3.3 示例：审核对文件夹失败的访问

1. 任务描述

test 文件夹拒绝 han 用户账户，启用审核策略，并且在 test 文件夹上审核 han 用户对该文件夹的访问。

2. 步骤

① 如图 9-7 所示，双击“审核对象访问”，选中“失败”复选框，单击“确定”按钮。

② 如图 9-8 所示，在 E 盘中创建一个文件夹 test，拒绝 han 用户读取和执行、列出文件夹目录和读取权限。

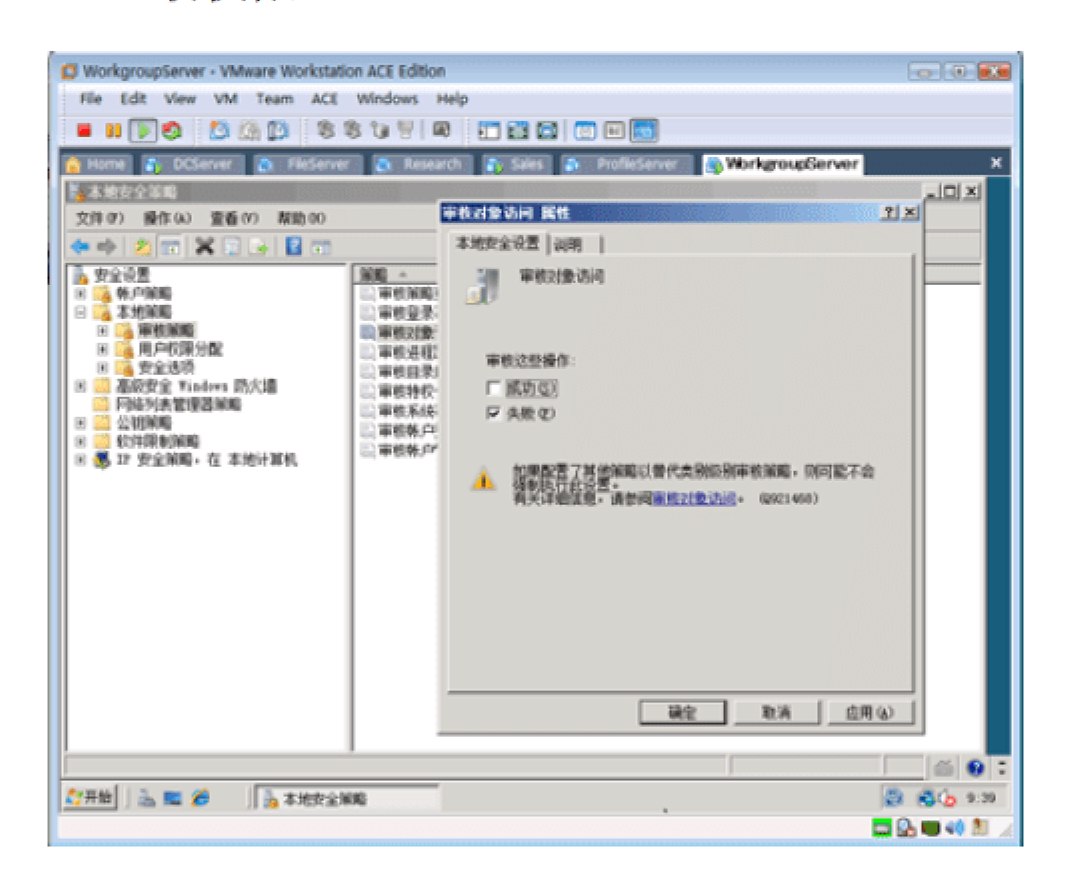


图 9-7 设置审核策略

图 9-8 在资源上设置审核(一)

③ 如图 9-9 所示，单击 test 文件夹属性“安全”选项卡中的“高级”按钮，在出现的对话框中，单击“审核”选项卡中的“编辑”按钮，单击“添加”按钮。

④ 如图 9-10 所示，在出现的选择用户对话框中，输入 han，单击“检查名称”按钮。

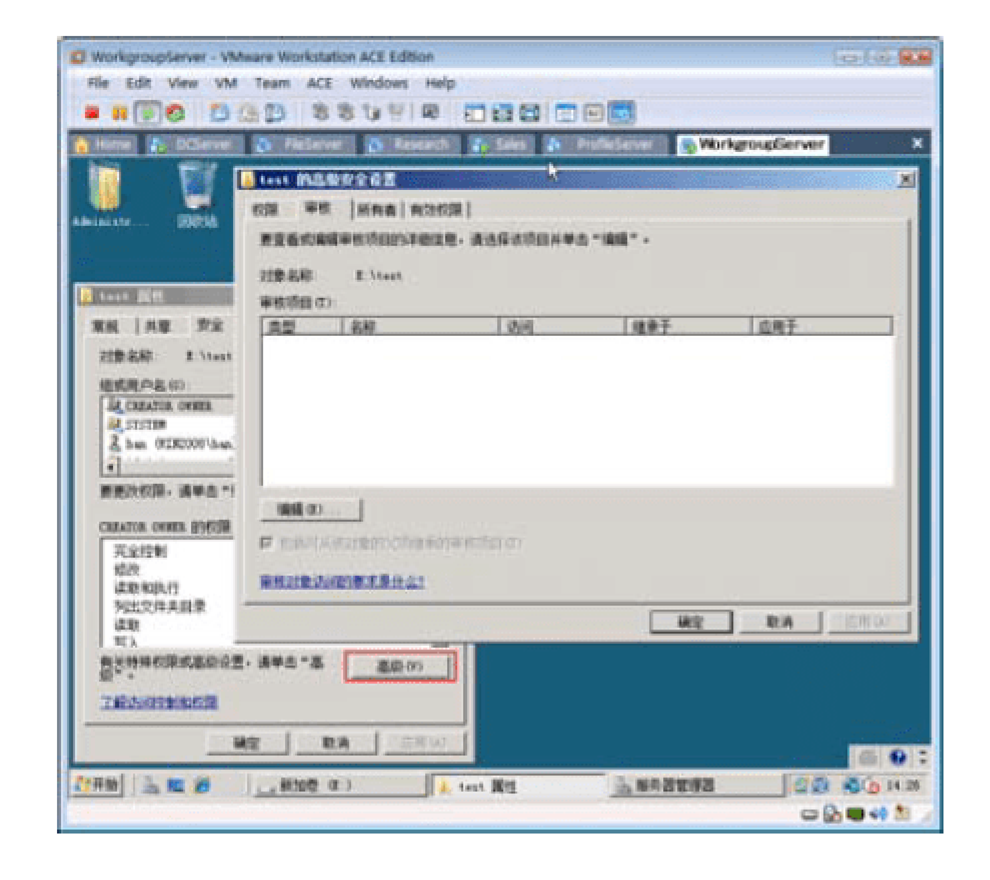


图 9-9 在资源上设置审核(二)

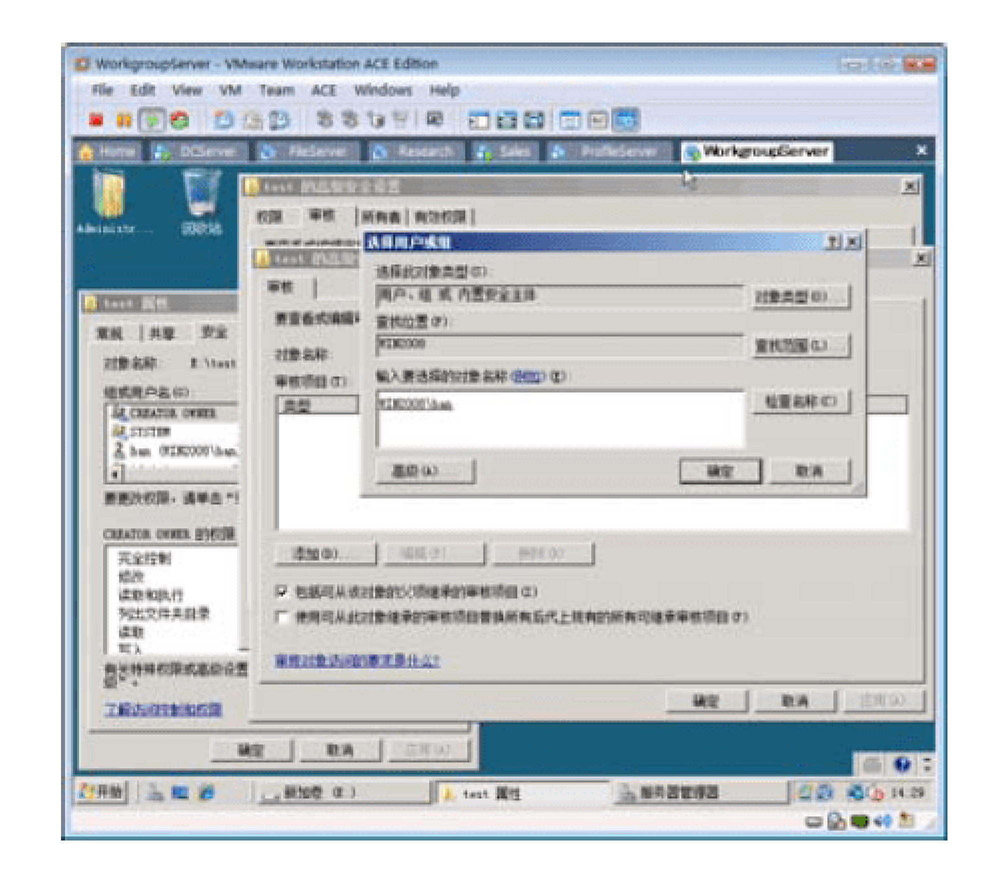


图 9-10 选择用户或组

⑤　出现如图 9-11 所示的对话框，在“列出文件夹/读取数据”右侧选中“失败”下的复选框。

⑥　如图 9-12 所示，切换用户，以 han 用户登录，双击 test 文件夹，被拒绝。

⑦　如图 9-13 所示，切换至管理员，查看日志。可以看到 han 用户访问 E:\test 文件夹审核失败。

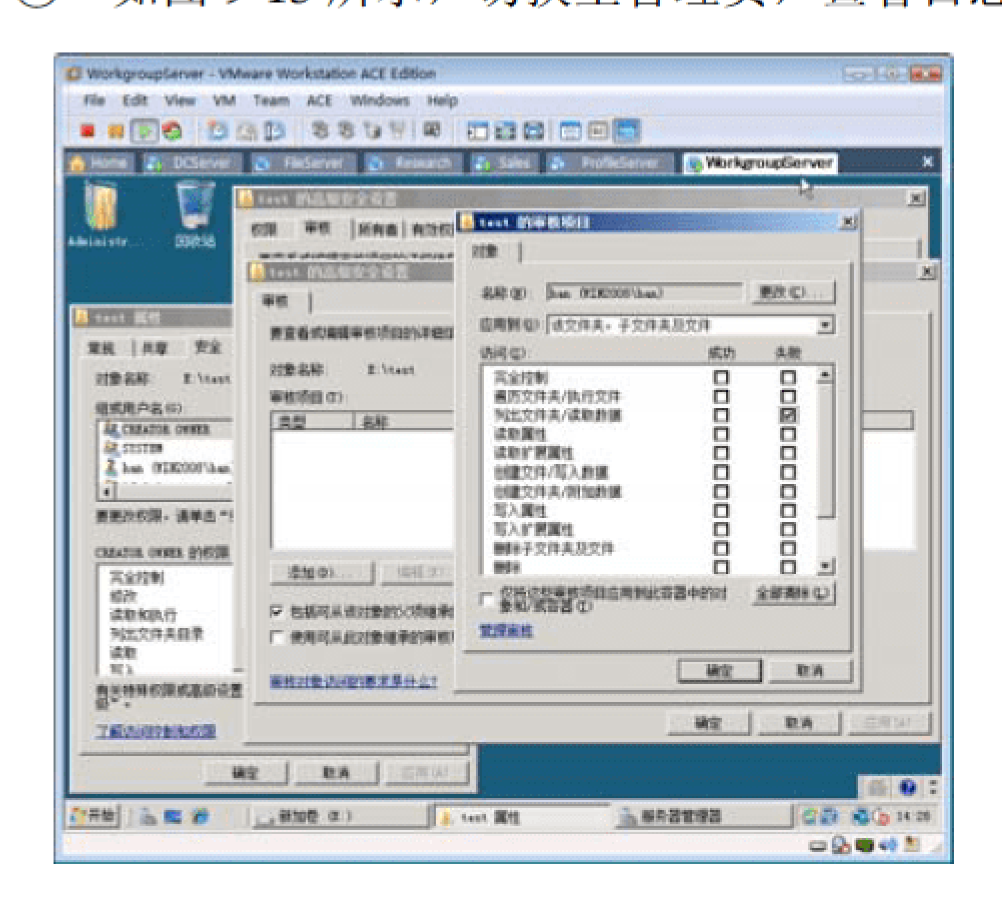




图 9-11　在资源上设置审核失败

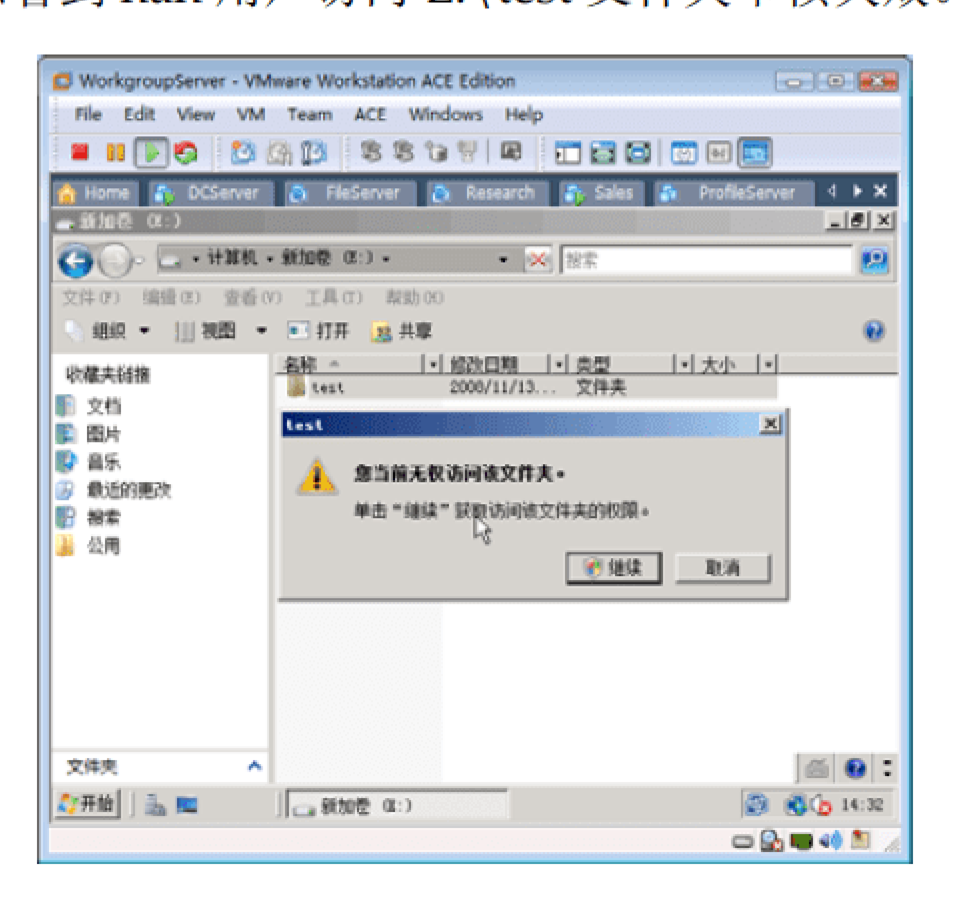


图 9-12　访问失败

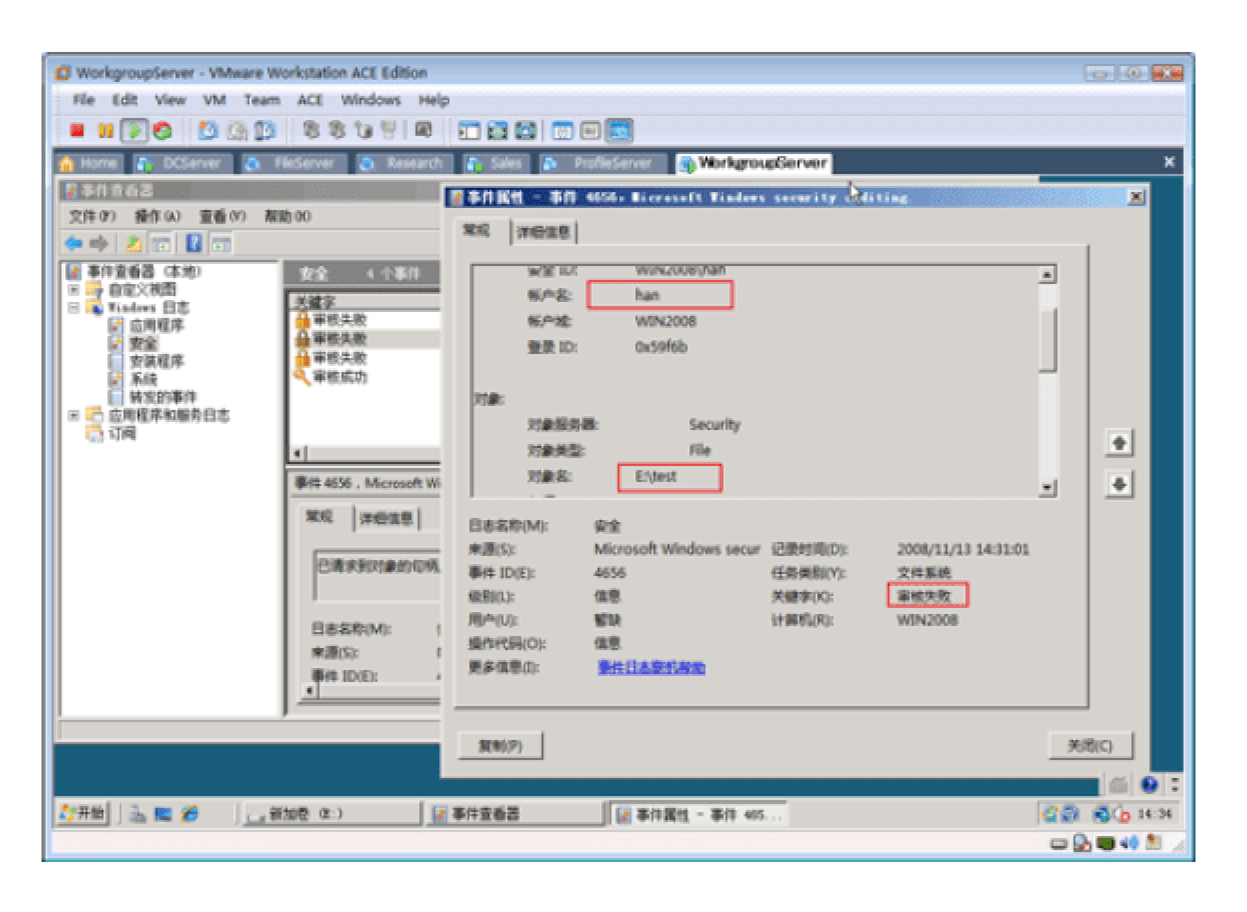


图 9-13　查看审核日志

9.3.4　示例：登录服务器失败，Windows Server 2008 自动报警

相信不少网络管理员都有过这样的经历：有时局域网服务器系统出现了一些莫名其妙的故障现象，查看对应系统的事件日志内容时，却发现事件日志中非常直观地指明了故障现象的具体原因。那能否让服务器系统自动报警，及时提醒网络管理员当前系统发生了重大事件呢?

在 Windows Server 2008 系统环境下，我们可以轻松地做到这一点。因为该系统已经将任务计划功能和事件查看器程序整合在一起，在事件查看器窗口中我们可以轻松针对一些重要事件添加报警任务，日后一旦重要事件发生时 Windows Server 2008 系统自然会自动报警了。

1. 自动报警思路

由于 Windows Server 2008 系统的自动报警功能只有基于某个特定的系统事件才能启用运行，不过

Windows Server 2008 系统在默认状态下不会自动记录下登录服务器失败的事件，为此我们应该先修改对应系统的审核策略，确保对登录服务器失败行为进行审核。接着退出服务器系统，并随意使用一个用户账号尝试登录 Windows Server 2008 系统，一旦登录失败时，对应系统的事件查看器中就会自动生成一个登录服务器失败的事件记录。之后，我们针对这个登录服务器失败的事件记录，附加一个发出报警的任务计划。当以后再有用户登录服务器失败时，那么对应该事件记录的任务计划就会被自动触发运行，此时网络管理员就能根据报警提示信息，及时采取措施来解决登录服务器失败故障现象了。

2. 任务审核登录失败操作

由于 Windows Server 2008 系统的日志功能在默认状态下不会自动记录服务器登录失败操作，必须先对这种操作进行安全审核，日后服务器系统才会对系统登录失败操作进行日志记录。在对服务器登录失败操作进行审核时，可以按照如下步骤来进行。

① 以超级管理员权限进入 Windows Server 2008 系统，从该系统桌面中打开“开始”菜单，并从中选择“运行”命令，打开系统“运行”对话框。

② 在其中输入字符串命令 secpol.msc，按 Enter 键，打开对应系统的本地安全策略列表窗口，如图 9-14 所示，设置审核登录事件失败。

③ 如此一来，Windows Server 2008 系统的日志功能日后就能对服务器登录失败操作进行自动记录了。

3. 创建登录失败事件

由于 Windows Server 2008 系统的自动报警功能是基于某一个特定事件的，为此需要自行创建一个服务器登录失败事件。在创建服务器登录失败事件时，我们只要先注销当前的服务器系统，之后随意使用一个不合法的用户账号尝试登录服务器系统，当系统提示登录失败时，Windows Server 2008 系统的日志功能就能将该事件记录保存下来了。此时，可以按照如下步骤来查看服务器登录失败事件。

① 以管理员账号登录，打开事件查看器，如图 9-15 所示，可以看到登录失败的日志记录。

② 此时可看到一个事件 ID 为 4625 的审核失败记录，双击该事件记录，从其后的界面中就能看到登录服务器失败的说明信息了。这说明服务器登录失败事件已经创建成功了。

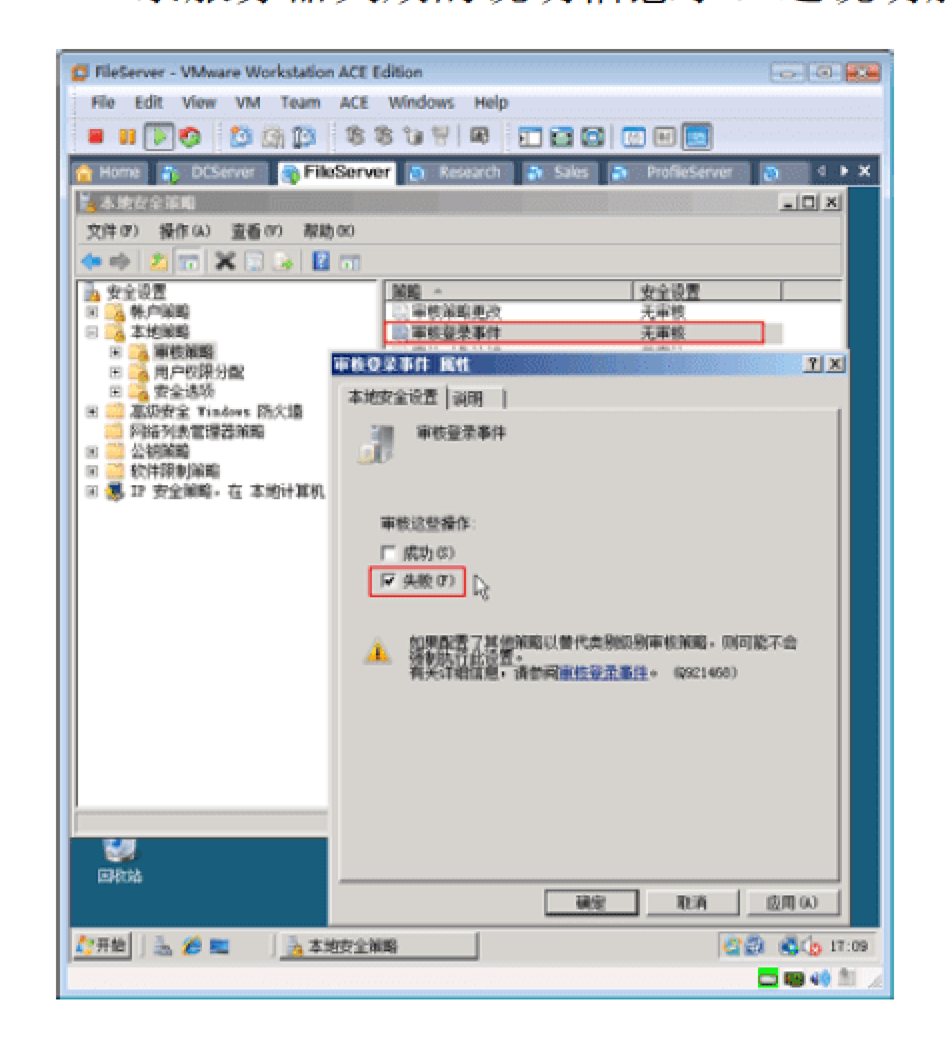


图 9-14　设置审核策略

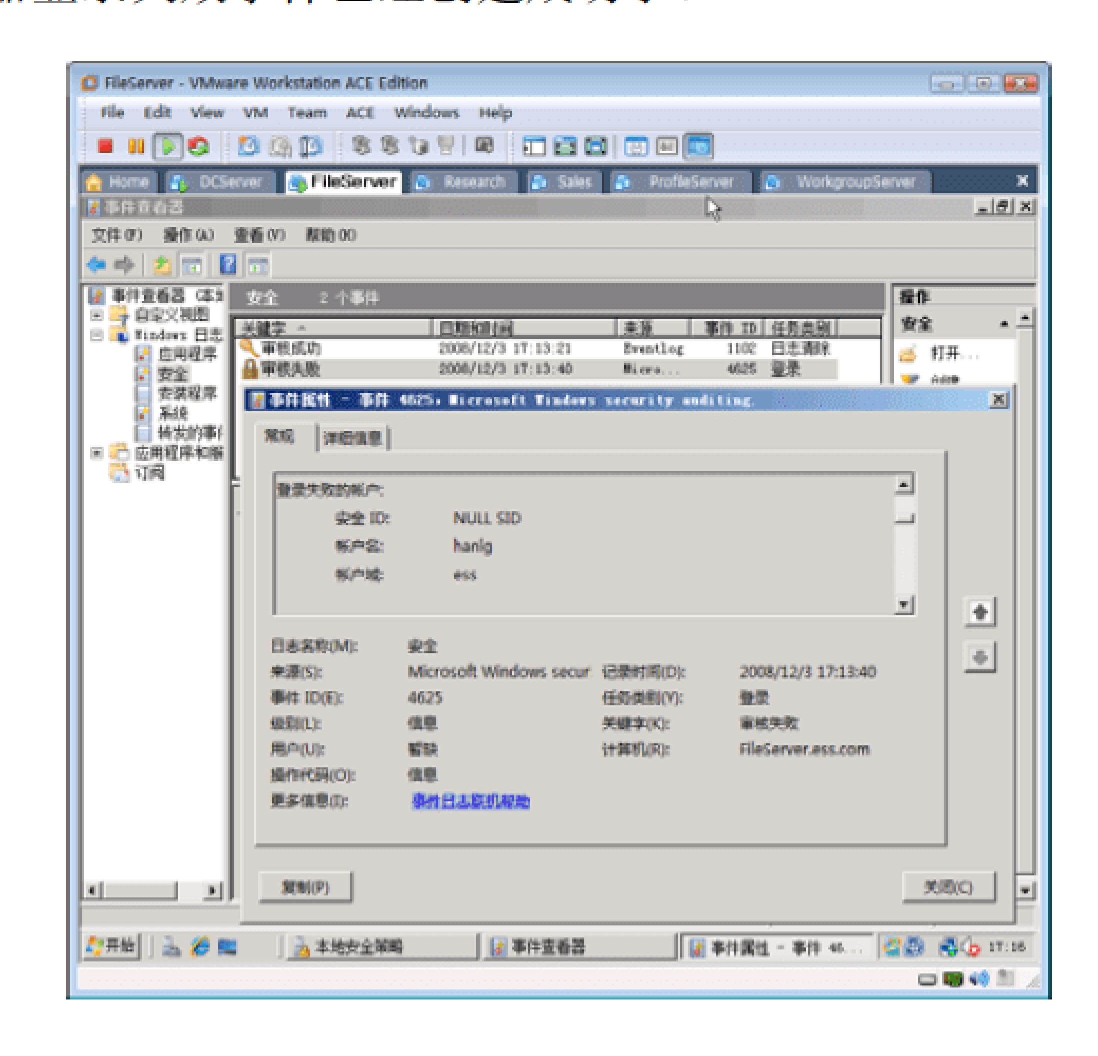


图 9-15　登录失败日志记录

4. 附加自动报警任务

与传统操作系统不一样的是，Windows Server 2008 系统可以针对某一个特定的事件记录附加运行任务计划。利用该功能可以将自动报警的任务计划附加到服务器登录失败事件中，一旦日后有用户再次遇到登录服务器失败操作时，网络管理员立即根据 Windows Server 2008 系统的自动报警提示来快速解决问题。在附加自动报警任务计划时，可以按照如下步骤来进行。

① 按照前面的操作步骤找到事件 ID 为 4625 的审核失败记录，右击该记录选项，从弹出的快捷菜单中执行“将任务附加到此事件”命令，如图 9-16 所示。当然，也可以直接单击右侧操作列表区域中的“将任务附加到此事件”选项，打开创建基本任务向导对话框。

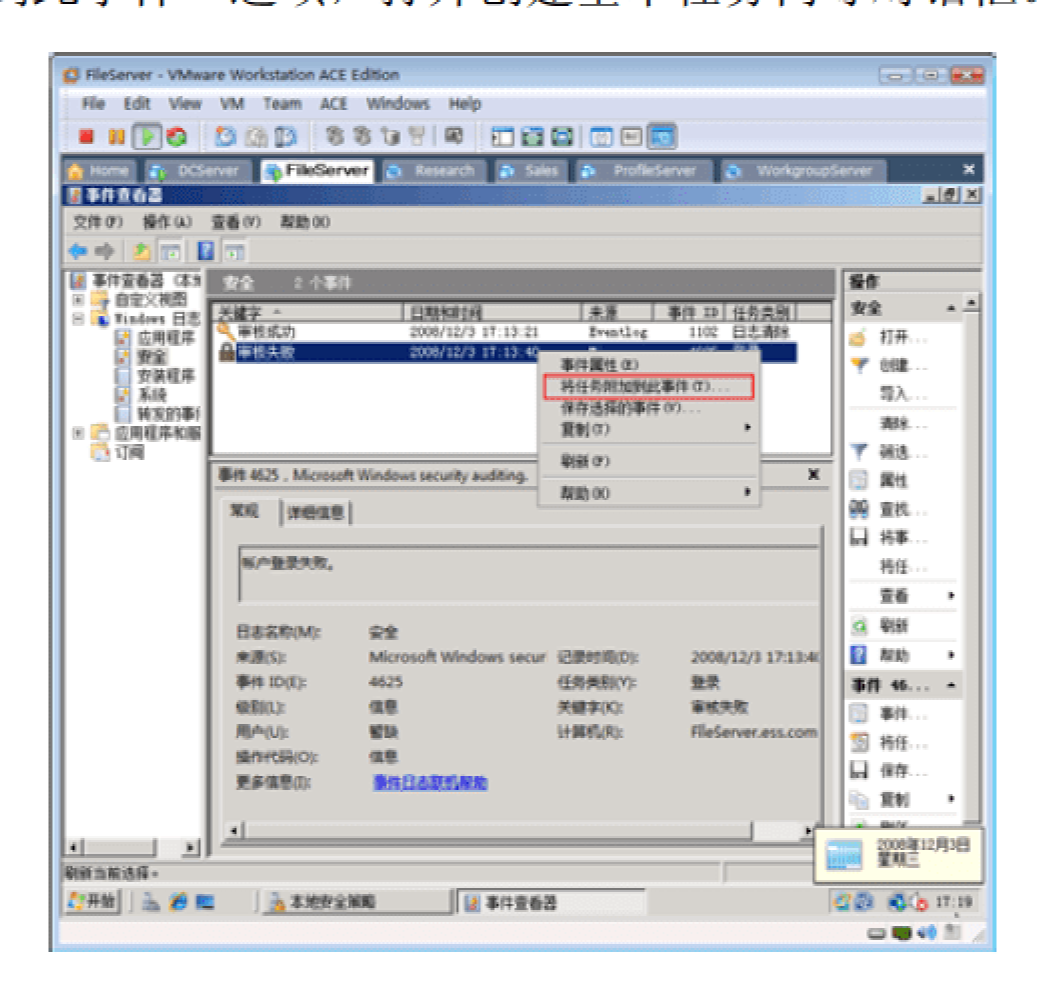


图 9-16 将任务附加到此事件

② 如图 9-17 所示，根据向导提示设置目标任务的名称，在这里将该任务名称取为“服务器登录失败报警”，之后连续单击“下一步”按钮。

③ 如图 9-18 所示，在“登录特定事件时”界面中，单击“下一步”按钮。

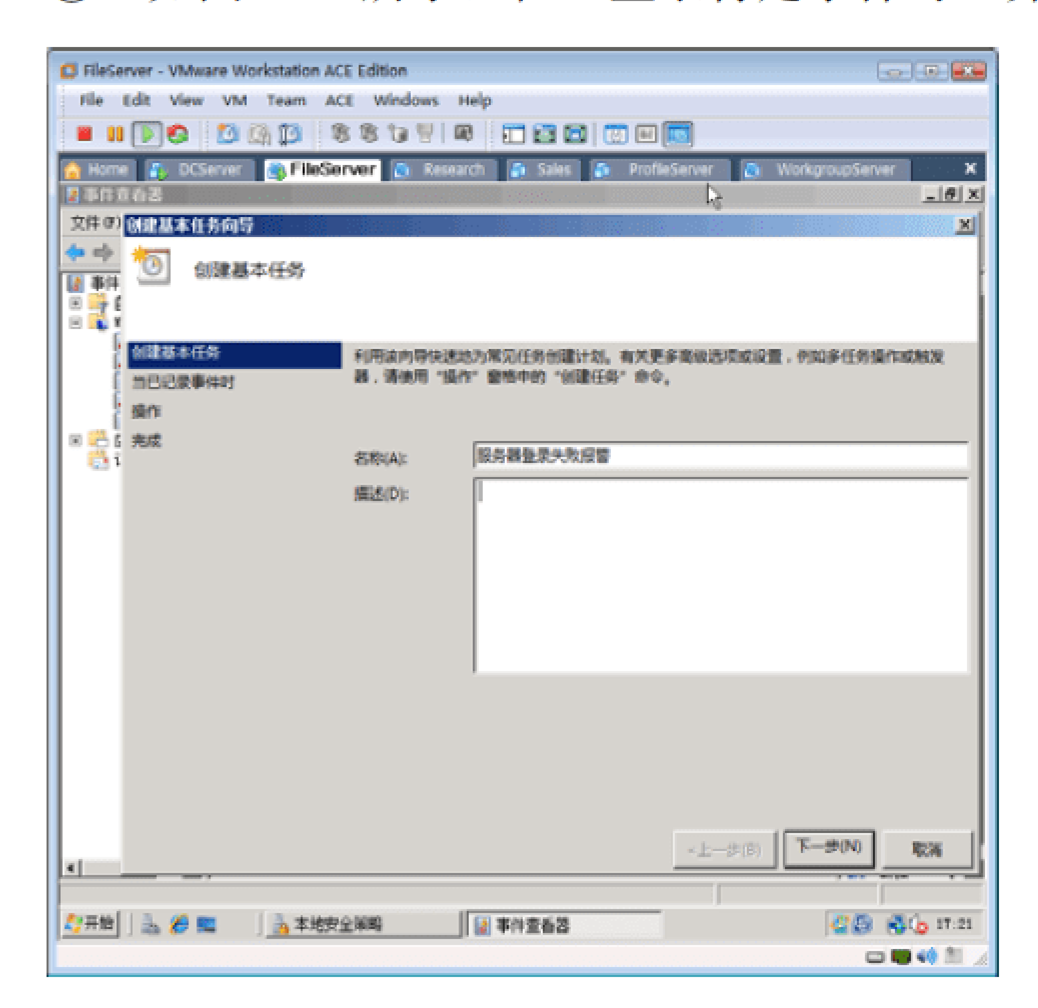


图 9-17 指定任务名称

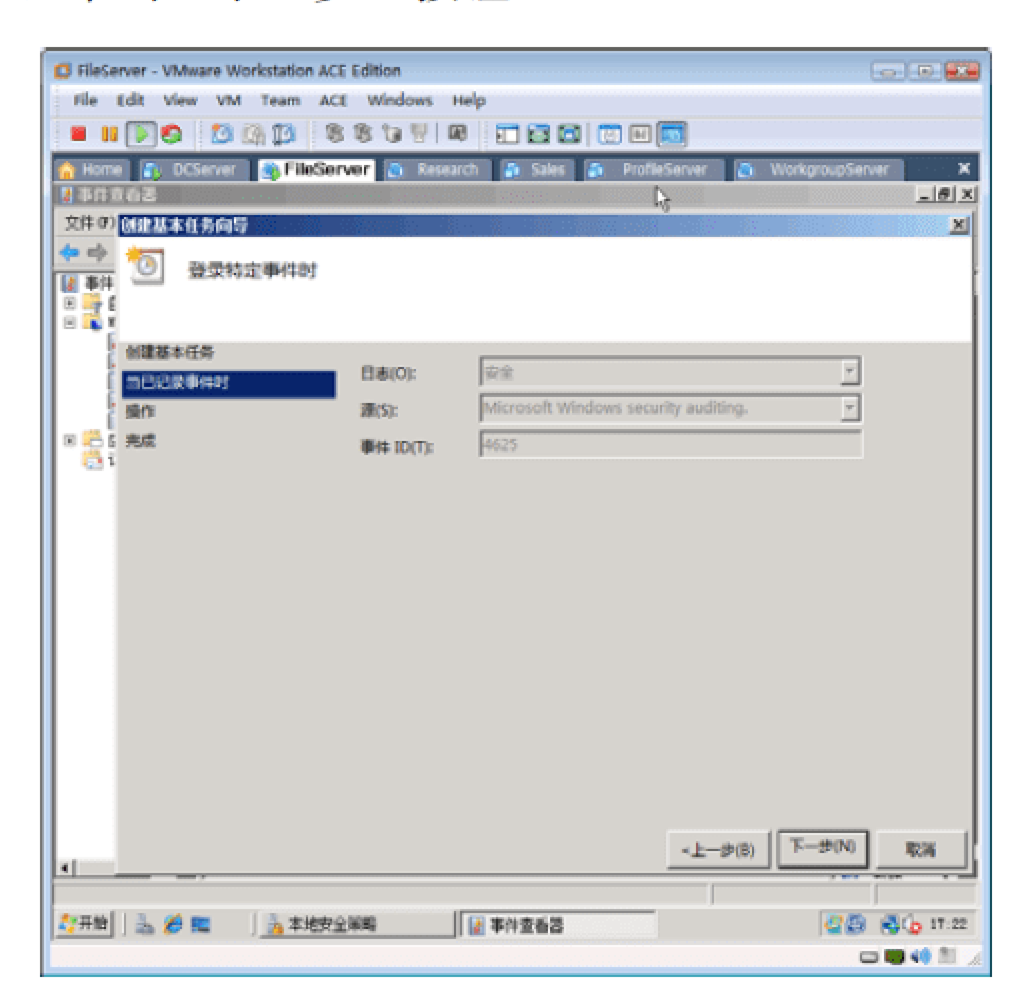


图 9-18 “登录特定事件时”界面

④ 在此界面中可发现 Windows Server 2008 系统为用户提供了 3 种操作选项，可以根据自己的喜好任意选择一种自动报警的方式，如图 9-19 所示，在这里选择“显示消息”单选按钮。

⑤ 继续单击“下一步“按钮，打开如图 9-20 所示的报警内容设置界面，在这里设置报警的标题以及内容信息，设定的内容日后会自动显示在报警提示对话框中。假设在这里将报警标题“服务器登录失败报警”内容设置为“当前有人登录服务器失败，请立即采取措施解决问题!”。

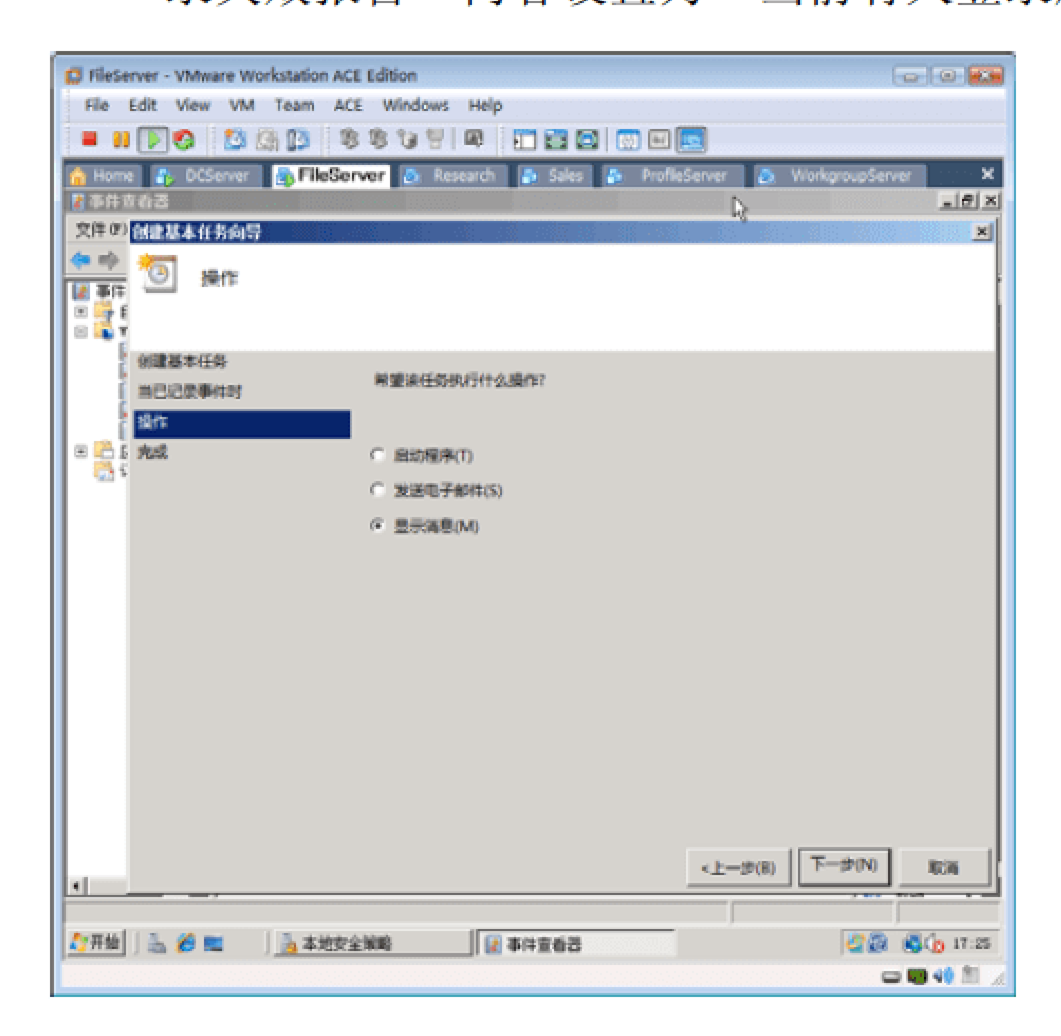


图 9-19　操作选项

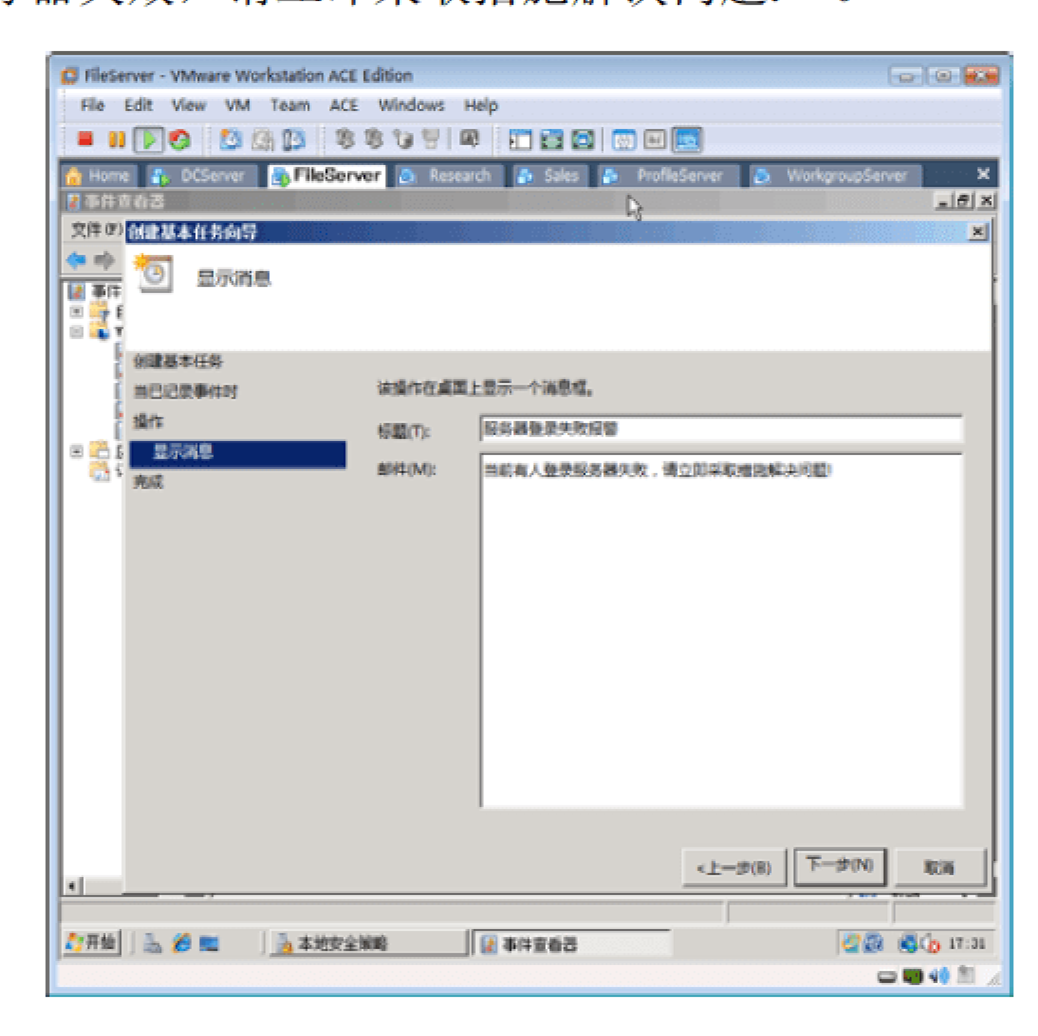


图 9-20　报警内容

⑥ 如图 9-21 所示选中“当单击(完成)时，打开此任务属性的对话框”复选框，如图 9-22 所示，可以看到已经创建了一个任务计划。

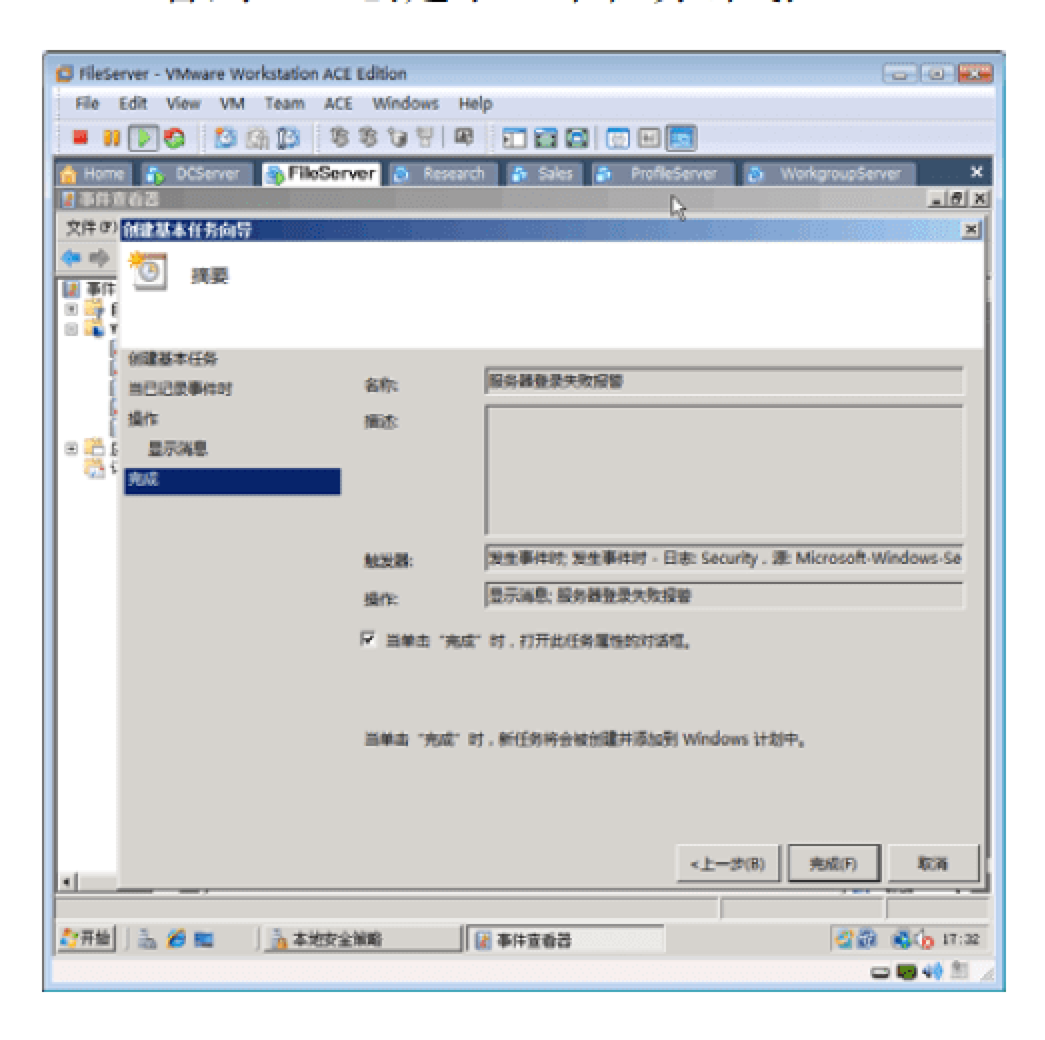


图 9-21　完成附加警报

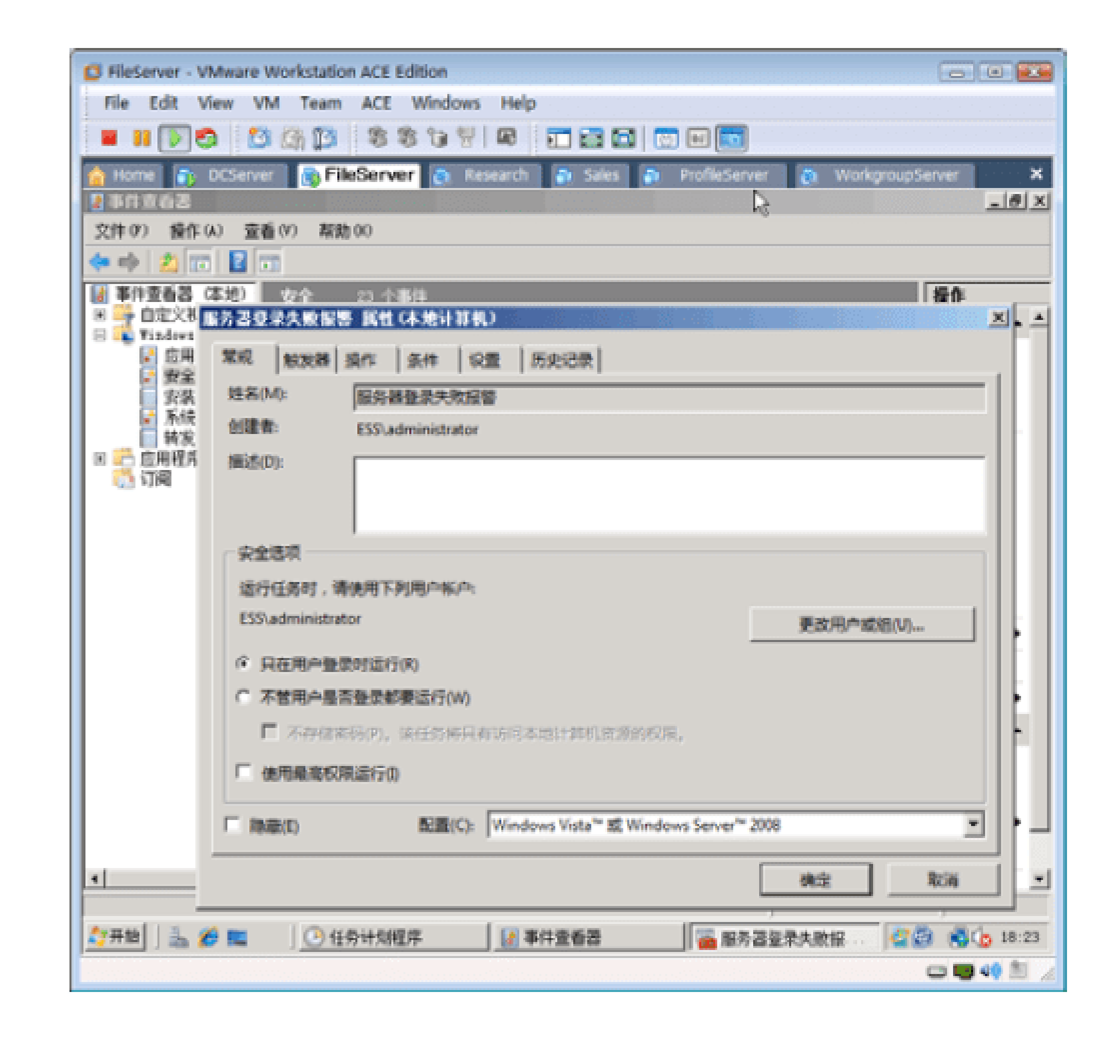


图 9-22　任务计划

⑦ 如图 9-23 所示，按 Ctrl+Alt+Insert 组合键，切换用户，输入一次错误的账号和密码，再输入正确的用户密码登录。可以看到登录后有消息提示框出现。

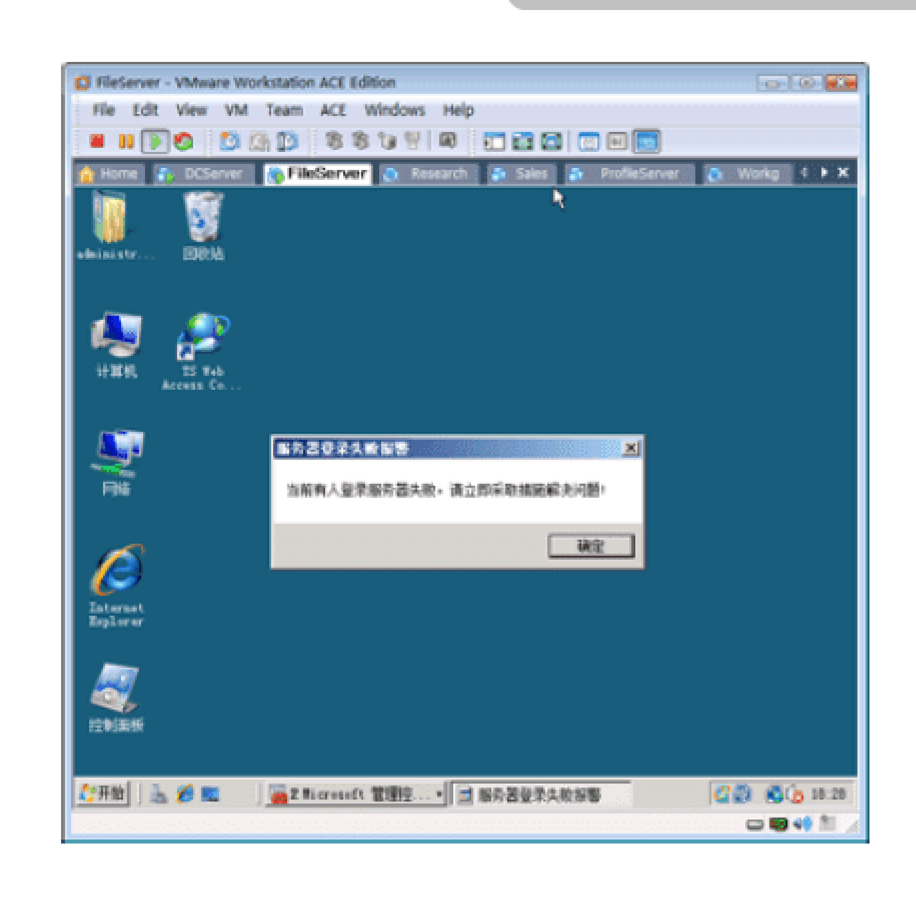


图 9-23　警报信息

9.4　用户权限分配

用户权限是允许用户在计算机系统或域中执行的任务。有两种类型的用户权限：登录权限和特权。

登录权限控制为谁授予登录计算机的权限以及他们的登录方式。特权控制对计算机上系统范围的资源的访问，并可以覆盖在特定对象上设置的权限。在本地登录计算机的权限就是一种登录权限。关闭系统的权限就是一种特权。这两种用户权限都由管理员作为计算机安全设置的一部分分配给单个用户或组。

9.4.1　用户权限设置

1. 允许本地登录

此登录权限确定哪些用户能以交互方式登录到此计算机。通过在连接的键盘上按 Ctrl+Alt+Del 组合键启动的登录要求用户具有此登录权限。此外，可以登录用户的某些服务或管理应用程序可能要求此登录权限。如果为某个用户或组定义此策略，则还必须向 Administrators 组授予此权限。

工作站和服务器上的默认值：Administrators、Backup Operators 和 Users。

域控制器上的默认值：Account Operators、Administrators、Backup Operators、Print Operators 及 Server Operators。

2. 关闭系统

此安全设置确定哪些在本地登录到计算机的用户可以使用关机命令来关闭操作系统。误用此用户权限会导致拒绝服务。

工作站上的默认值：Administrators、Backup Operators 及 Users。

服务器上的默认值：Administrators 和 Backup Operators。

域控制器上的默认值：Administrators、Backup Operators、Server Operators 及 Print Operators。

3. 从网络访问此计算机

此用户权限确定允许哪些用户和组通过网络连接到计算机。此用户权限不影响终端服务。

工作站和服务器上的默认值：Administrators、Backup Operators、Users 及 Everyone。

域控制器上的默认值：Administrators、Authenticated Users、Enterprise Domain Controllers、Everyone 及 Pre-Windows 2000 Compatible Access。

9.4.2 示例：拒绝本地登录

WorkgroupServer 是一个文件服务器，只允许使用 han 用户账户从网络访问该服务器中的资源，但拒绝 han 用户账户在本地登录。

① 如图 9-24 所示，在 WorkgroupServer 上拒绝 han 用户本地登录。

② 如图 9-25 所示，双击“从网络访问此计算机”，删除现有的用户，添加 han 用户账号。

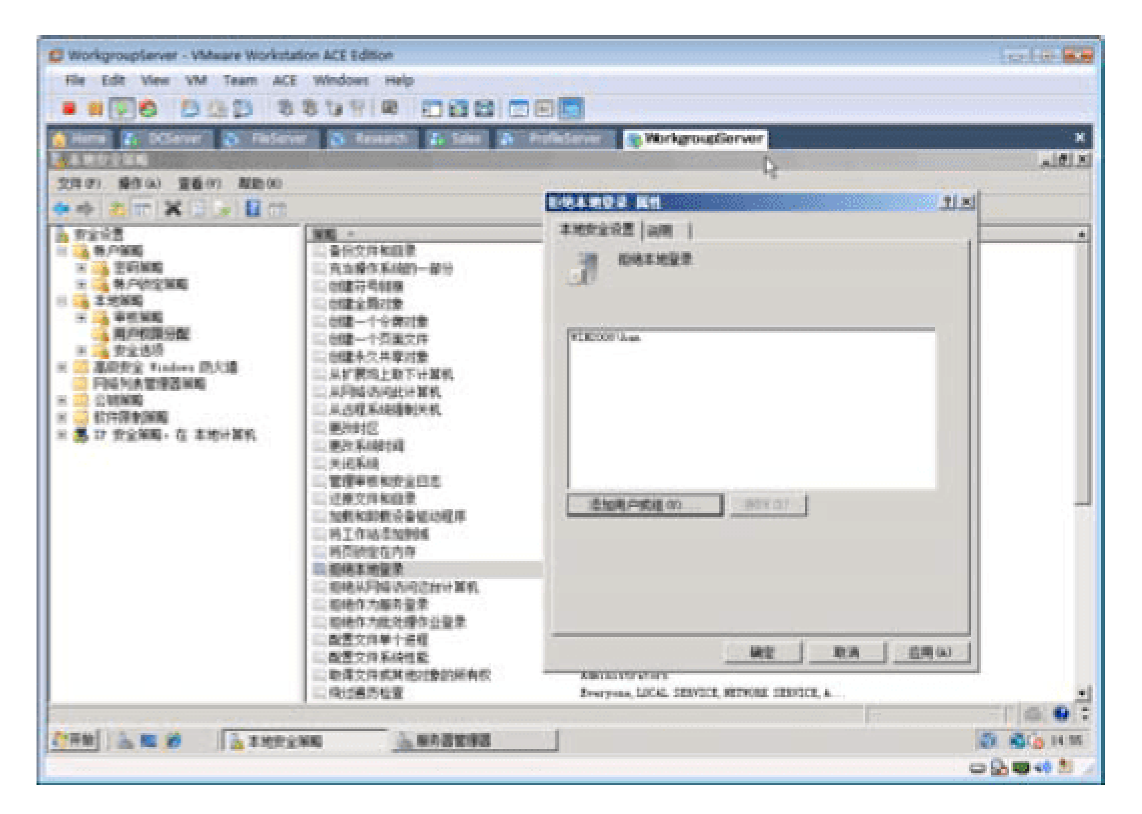


图 9-24 拒绝本地登录

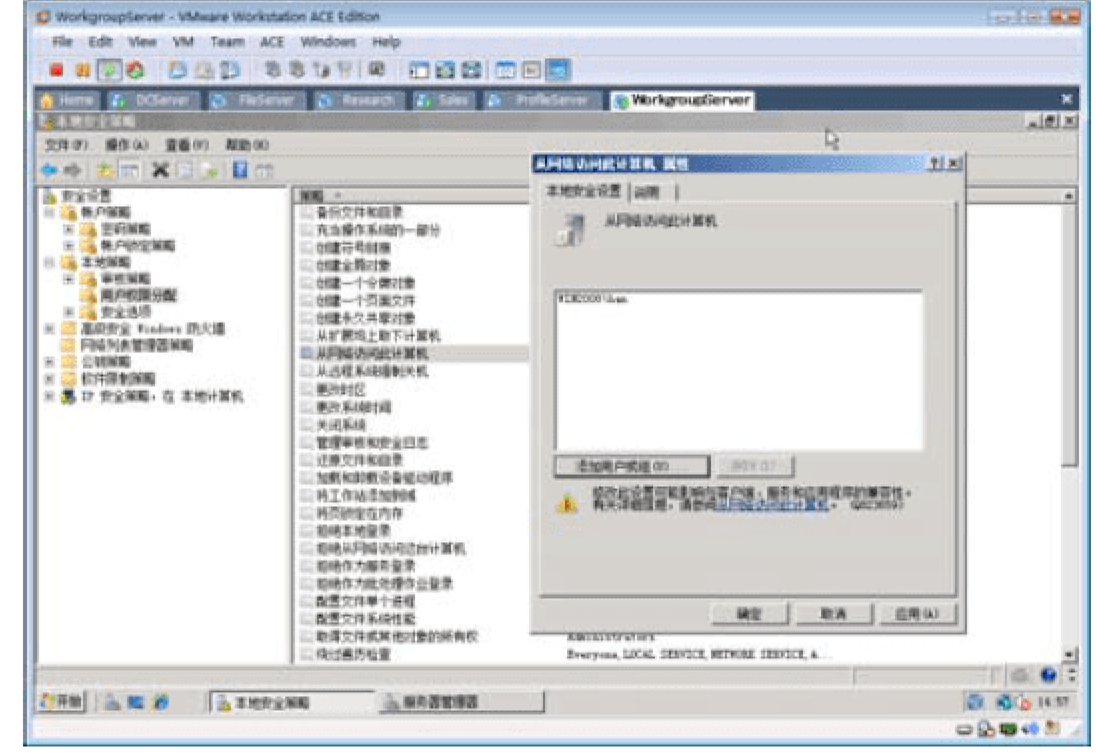
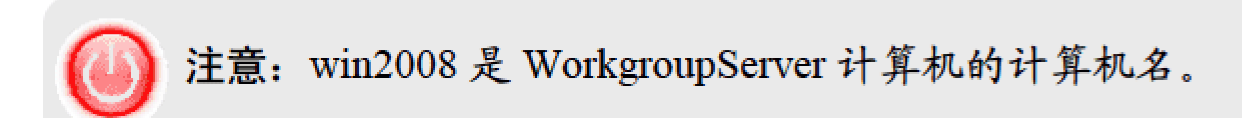


图 9-25 允许从网络访问计算机

③ 在 Sales 计算机上访问 WorkgroupServer 计算机的共享名，输入 win2008\han 和密码，能够访问 WorkgroupServer 共享文件，如图 9-26 所示。



注意：win2008 是 WorkgroupServer 计算机的计算机名。

④ 如图 9-27 所示，在 WorkgroupServer 计算机上，切换用户，发现已经没有 han 用户账户列出。

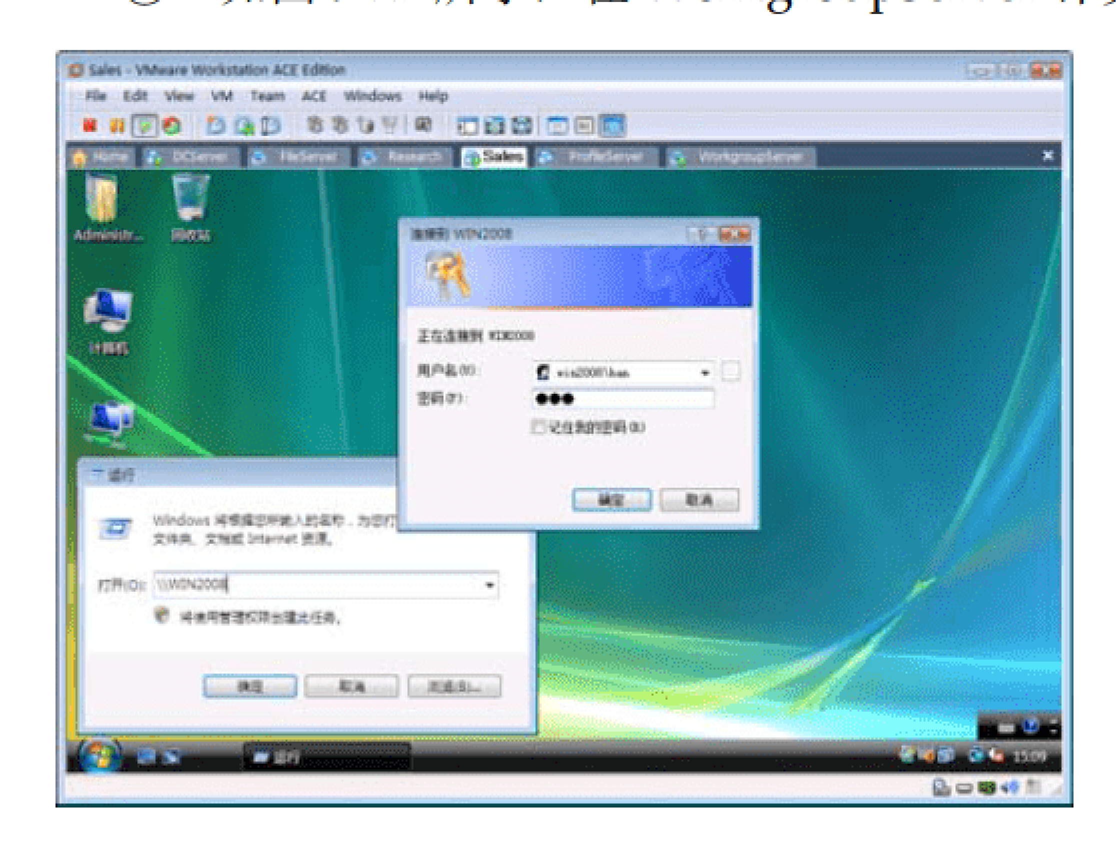


图 9-26 从网络访问服务器

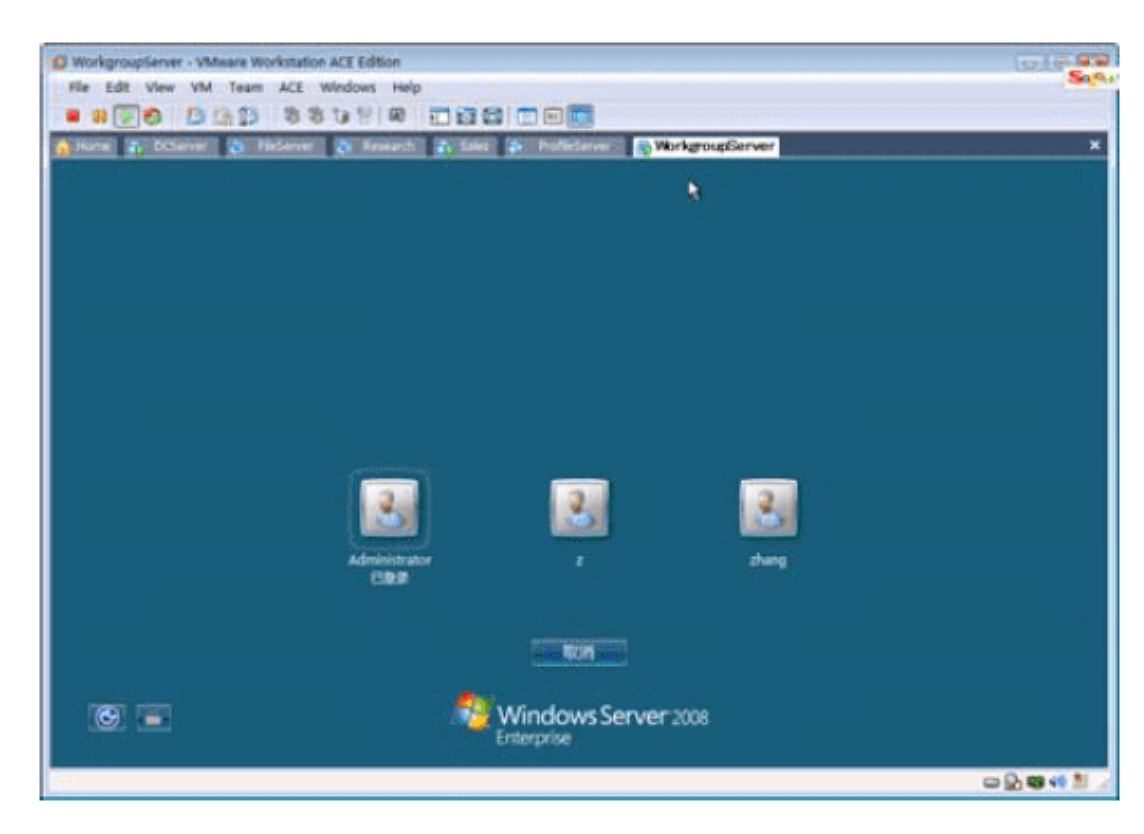


图 9-27 本地登录不出现 han 用户

9.5 安 全 选 项

9.5.1 安全选项设置

1. 交互式登录：不显示最后的用户名

该安全设置确定是否在 Windows 登录屏幕中显示最后登录到计算机的用户的名称。

如果启用该策略，则不会在“登录到 Windows”对话框中显示最后成功登录的用户的名称；

如果禁用该策略，则显示最后登录的用户的名称。

默认：禁用。

2. 交互式登录：提示用户在密码过期之前进行更改

确定提前多长时间(以天为单位)向用户发出其密码即将过期的警告。借助该提前警告，用户有时间构造足够强大的密码。

默认：14 天。

3. 审核：如果无法记录安全审核则立即关闭系统

此安全设置确定无法记录安全事件时系统是否会关机。

启用此安全设置后，如果因任何原因无法记录安全审核，它就会停止系统。通常，当安全审核日志已满且为安全日志指定的保留方法为“不覆盖事件”或“按天数覆盖事件”时，会无法记录事件。

如果安全日志已满且无法覆盖某个现有条目，并且启用了此安全选项，则会出现下列停止错误：

```
STOP：C0000244 {审核失败}
```

尝试生成安全审核失败。

若要恢复，管理员必须根据需要登录、归档日志(可选)、清除日志以及重置此选项。即使安全日志未满，也要到重置此安全设置之后，非 Administrators 组成员用户才能登录到系统。



注意：配置此安全设置时，只有重新启动 Windows，更改才会生效。

默认：禁用。

4. 网络访问：本地账户的共享和安全模型

此安全设置确定如何对使用本地账户的网络登录进行身份验证。如果将此设置设为“经典”，使用本地账户凭据的网络登录通过这些凭据进行身份验证。“经典”模型允许更好地控制对资源的过度访问。通过使用“经典”模型，可以针对同一个资源为不同用户授予不同的访问类型。

如果将此设置设为“仅来宾”，使用本地账户的网络登录会自动映射到来宾账户。通过使用“仅来宾”模型，可以平等地对待所有用户。以来宾身份验证所有用户，使所有用户都获得相同的访问权限级别来访问指定的资源，这些权限可以为只读或修改。

在域计算机上的默认设置：经典。

在独立计算机上的默认设置：仅来宾。



提示：

- 使用“仅来宾”模型时，所有可以通过网络访问计算机的用户(包括匿名 Internet 用户)都可以访问共享资源。你必须使用 Windows 防火墙或其他类似设备来防止对计算机进行未经授权的访问。同样，使用“经典”模型时，本地账户必须受密码保护，否则，这些用户账户可以被任何人用来访问共享的系统资源。
- 此设置不会影响通过使用如 Telnet 或终端服务等服务远程执行的交互式登录。此策略将不会影响运行 Windows 2000 的计算机。计算机未加入域时，此设置也会将 Windows 资源管理器中的“共享和安全”选项卡修改为与正在使用的共享和安全模型对应的设置。

9.5.2 示例：不显示最后的用户名

为确保服务器安全，不显示最后的用户名。

① 如图 9-28 所示，默认登录时，按 Ctrl+Alt+Delete 组合键，将显示所有的用户名。

② 如图 9-29 所示，双击“交互式登录: 不显示最后的用户名”，选中“已启用”单选按钮。

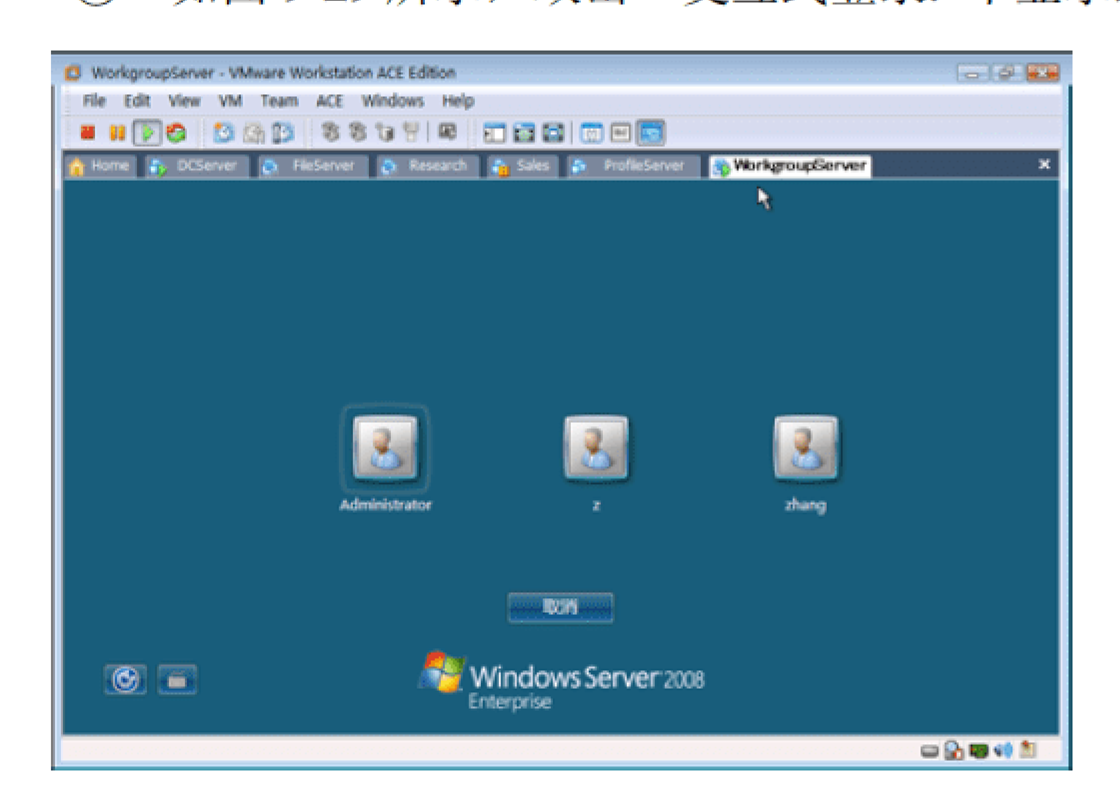


图 9-28 显示所有用户

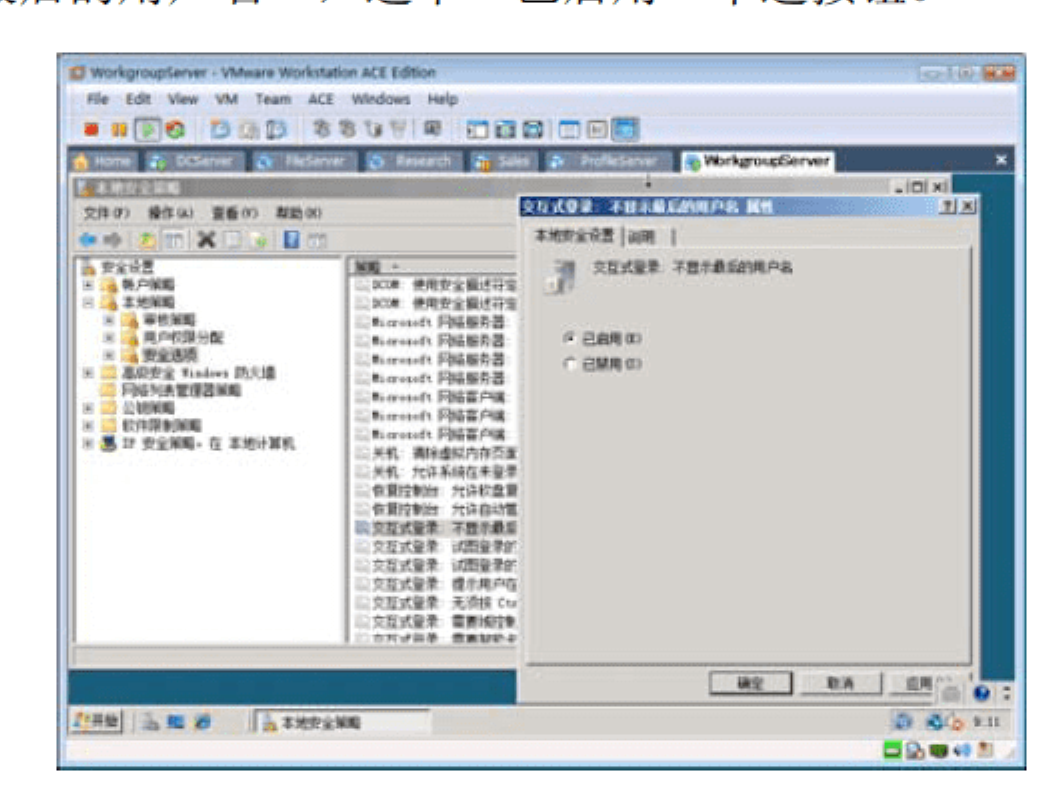


图 9-29 不显示登录名(一)

③ 如图 9-30 所示，登录时将不会显示该计算机上的所有用户名。

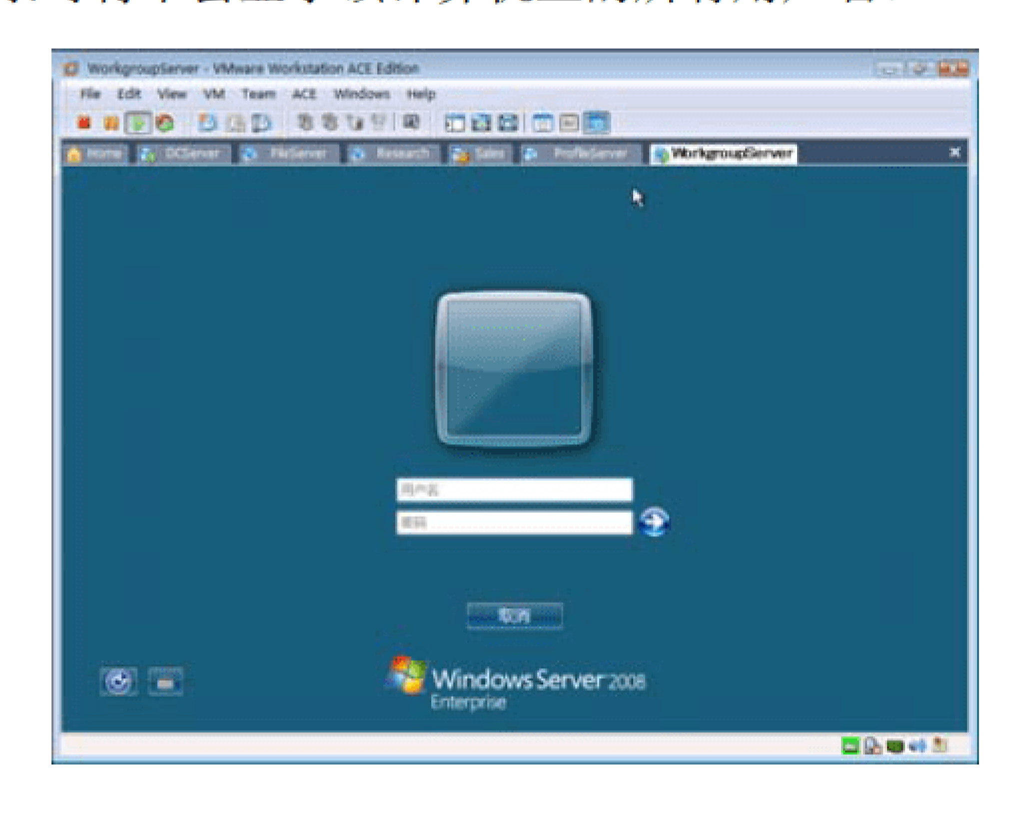


图 9-30 不显示登录名(二)

9.5.3　示例：只允许使用 Guest 账户访问

① 如图 9-31 所示，双击“网络访问：本地帐户的共享和安全模型”，选中“仅来宾—对本地用户进行身份验证，其身份为来宾”选项。

注意：如果启用“仅来宾”，必须启用 Guest 账户。Guest 账户的密码默认为空。如果 Guest 帐户密码为空，用户访问 WorkgourpServer 时，不需要输入账号和密码，直接以 Guest 账户连接该服务器即可。

② 如图 9-32 所示，展开“服务器管理器”→“配置”→“本地用户和组”→“用户”节点，在右侧的窗格中双击 Guest 账户，在用户属性对话框中，取消选中“帐户已禁用”复选框，单击“确定”按钮。

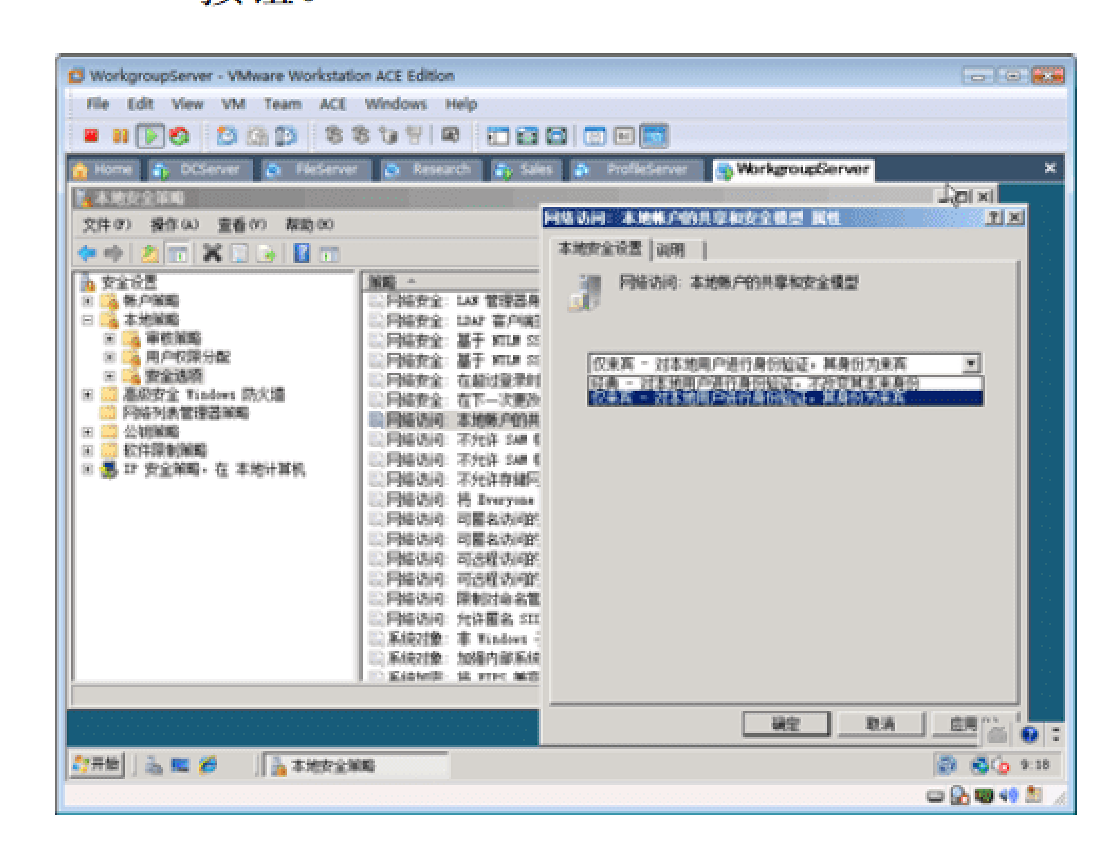


图 9-31　本地账户的共享和安全模型

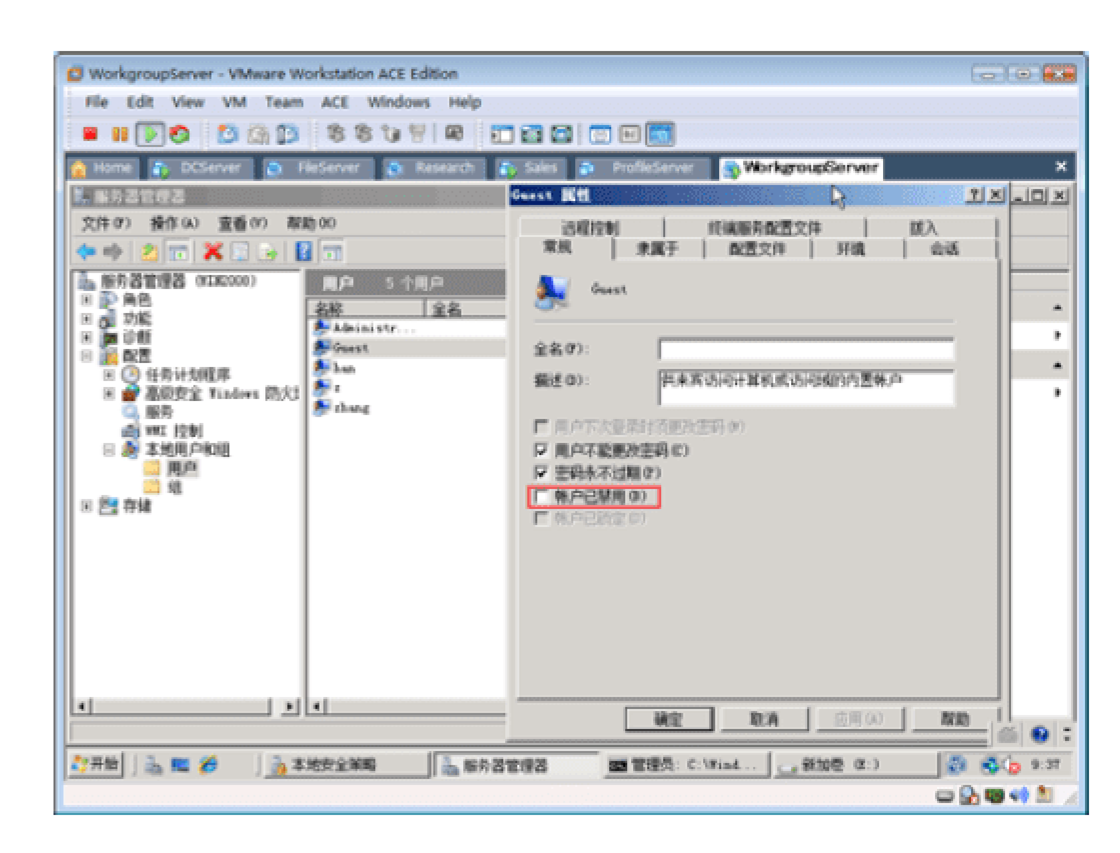


图 9-32　启用 Guest 账户

③ 如图 9-33 所示，在 Sales 计算机上访问 WorkgroupServer 计算机中的共享资源。此时会发现不需要输入任何凭据，就可以访问 WorkgroupServer 计算机中的共享文件和打印机。因为 Guest 账户密码为空。

④ 如图 9-34 所示，如果 Guest 账户有密码，则必须输入 Guest 账户以及密码才能访问。不允许使用其他用户账户访问 WorkgroupServer。

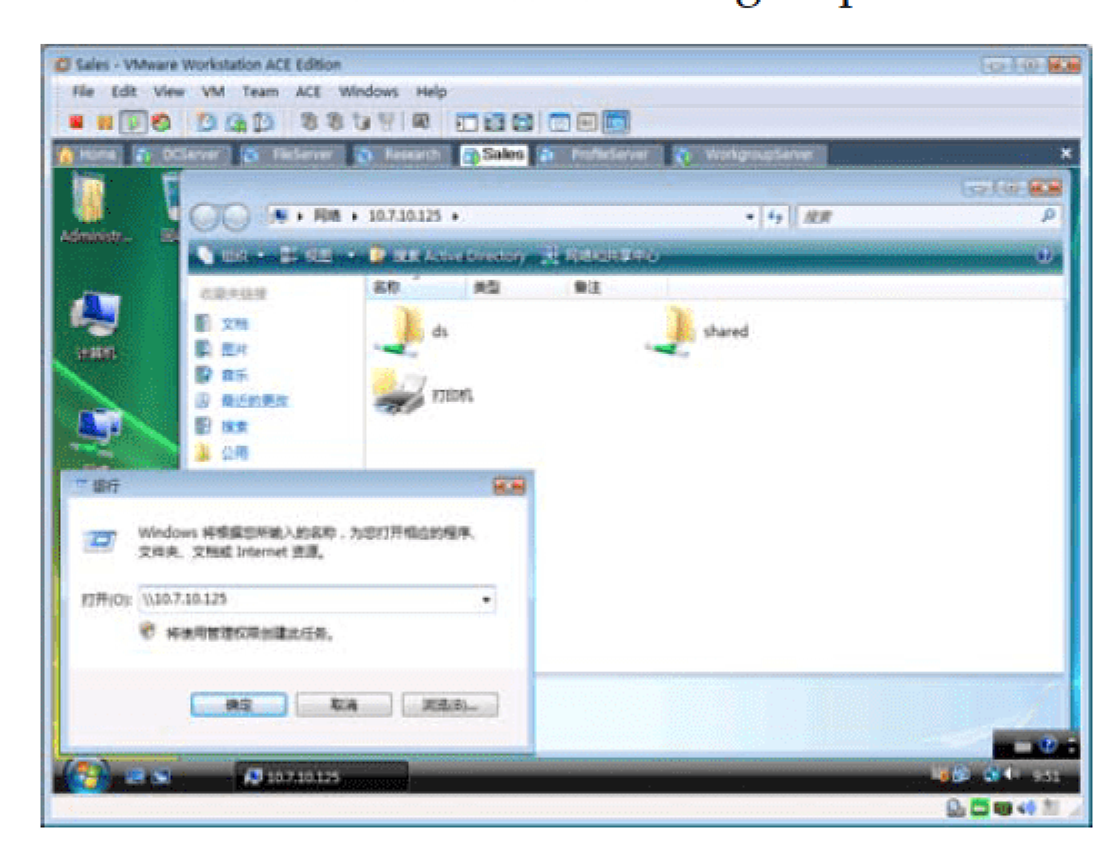


图 9-33　以 Guest 身份访问服务器

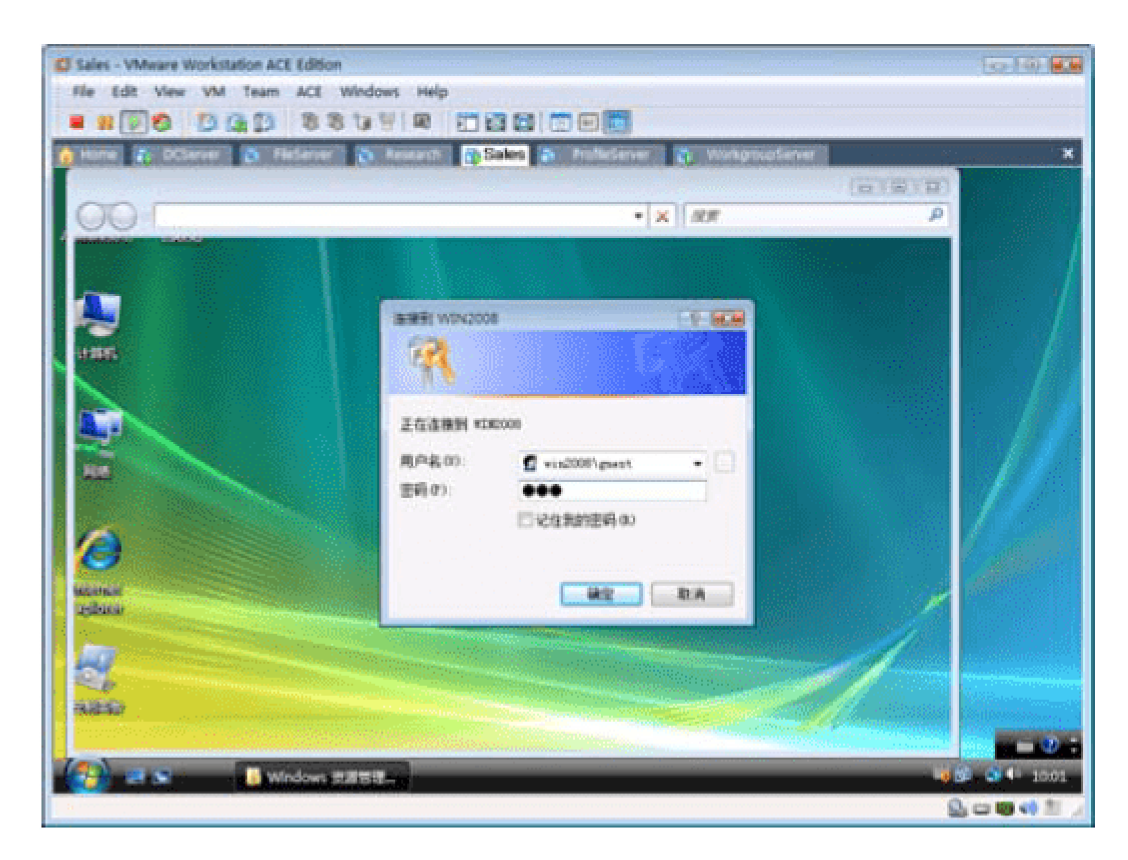


图 9-34　输入 Guest 密码

9.6 高级 Windows 防火墙

本节主要介绍具有高级安全性的 Windows 防火墙。其中包括有关防火墙的定义、运行方式和可以用于配置具有高级安全性的 Windows 防火墙和 Internet 协议安全 (IPSec) 设置的工具的概念性信息。

9.6.1 高级 Windows 防火墙简介

1. 具有高级安全性的 Windows 防火墙

具有高级安全性的 Windows 防火墙结合了主机防火墙和 IPSec。与边界防火墙不同，具有高级安全性的 Windows 防火墙在每台运行此版本 Windows 的计算机上运行，并对可能穿越外围网络或源于组织内部的网络攻击提供本地保护。它还提供计算机到计算机的连接安全，使用户可以对通信要求身份验证和数据保护。

具有高级安全性的 Windows 防火墙是一种状态防火墙，检查并筛选 IP 版本 4 (IPv4) 和 IP 版本 6 (IPv6) 流量的所有数据包。默认情况下阻止传入流量，除非是对主机请求(请求的流量)的响应，或者被特别允许(即创建了防火墙规则允许该流量)。通过配置具有高级安全性的 Windows 防火墙设置(指定端口号、应用程序名称、服务名称或其他标准)，可以显式允许流量。

使用具有高级安全性的 Windows 防火墙还可以请求或要求计算机在通信之前互相进行身份验证，并在通信时使用数据完整性或数据加密。

2. 高级安全性的 Windows 防火墙工作方式

具有高级安全性的 Windows 防火墙使用两组规则配置其如何响应传入和传出流量。防火墙规则确定允许或阻止哪种流量。连接安全规则确定如何保护此计算机和其他计算机之间的流量。通过使用防火墙配置文件(根据计算机连接的位置应用)，可以应用这些规则以及其他设置，还可以监视防火墙活动和规则。

3. 防火墙规则

配置防火墙规则以确定阻止还是允许流量通过具有高级安全性的 Windows 防火墙。传入数据包到达计算机时，具有高级安全性的 Windows 防火墙检查该数据包，并确定它是否符合防火墙规则中指定的标准。如果数据包与规则中的标准匹配，则具有高级安全性的 Windows 防火墙执行规则中指定的操作，即阻止连接或允许连接。如果数据包与规则中的标准不匹配，则具有高级安全性的 Windows 防火墙丢弃该数据包，并在防火墙日志文件中创建条目(如果启用了日志记录)。

对规则进行配置时，可以从各种标准中进行选择：例如应用程序名称、系统服务名称、TCP 端口、UDP 端口、本地 IP 地址、远程 IP 地址、配置文件、接口类型(如网络适配器)、用户、用户组、计算机、计算机组、协议及 ICMP 类型等。规则中的标准添加在一起；添加的标准越多，具有高级安全性的 Windows 防火墙匹配传入流量就越精细。

4. 连接安全规则

可以使用连接安全规则来配置本计算机与其他计算机之间特定连接的 IPSec 设置。具有高级安全性的 Windows 防火墙使用该规则来评估网络通信，然后根据该规则中所建立的标准阻止或允许消息。在某些

环境下具有高级安全性的 Windows 防火墙将阻止通信。如果所配置的设置要求连接安全(双向)，而两台计算机无法互相进行身份验证，则将阻止连接。

9.6.2 防火墙配置文件

可以将防火墙规则和连接安全规则以及其他设置应用于一个或多个防火墙配置文件。然后将这些配置文件应用于计算机，这取决于连接计算机的位置。可以配置计算机何时连接到域、专用网络(例如家庭网络)或公用网络(例如 Internet 展台)的配置文件。

防火墙配置文件是对根据连接计算机的位置应用于计算机的设置(如防火墙规则和连接安全规则)进行分组的方式。在运行此版本的 Windows 计算机上，具有高级安全性的 Windows 防火墙有 3 个配置文件。一次只能应用一个配置文件。

配置文件

- 域：当计算机连接到该计算机域账户所在的网络时应用。
- 专用：当计算机连接到没有该计算机域账户的网络(例如家庭网络)时应用。专用配置文件设置应比域配置文件设置更为严格。
- 公用：当计算机通过公用网络(如机场和咖啡店中的可用网络)连接到域时应用。由于计算机所连接到的公用网络无法像 IT 环境中一样严格控制安全，因此公用配置文件设置应最为严格。

9.6.3 示例：创建一个在企业内网使用的防火墙

你的笔记本电脑有两个工作环境，在企业内网和公共场所。企业内网是一个较为安全的网络环境。下面将针对较为安全的场所配置防火墙。

1. 配置目标

- 更改网络位置。
- 启用网络发现。
- 允许访问该计算机的共享文件夹。

2. 实战环境

WorkgroupServer，安装了 Windows Server 2008 企业版的操作系统，处于工作组中。

3. 步骤

① 在 WorkgroupServer 计算机上。

② 选择“开始”→“程序”→“管理工具”→“高级安全 Windows 防火墙”命令。在随后打开的对话框中，单击“本地计算机上的高级安全 Windows 防火墙”选项，可以看到公用配置文件是活动。

③ 单击按钮，单击“网络和共享中心”选项，如图 9-35 所示。

④ 如图 9-36 所示，在出现的“网络和共享中心”窗口中，单击“自定义”按钮。

⑤ 在出现的“设置网络位置”对话框中，选中“专用”单选按钮，单击“下一步”按钮，完成设置。

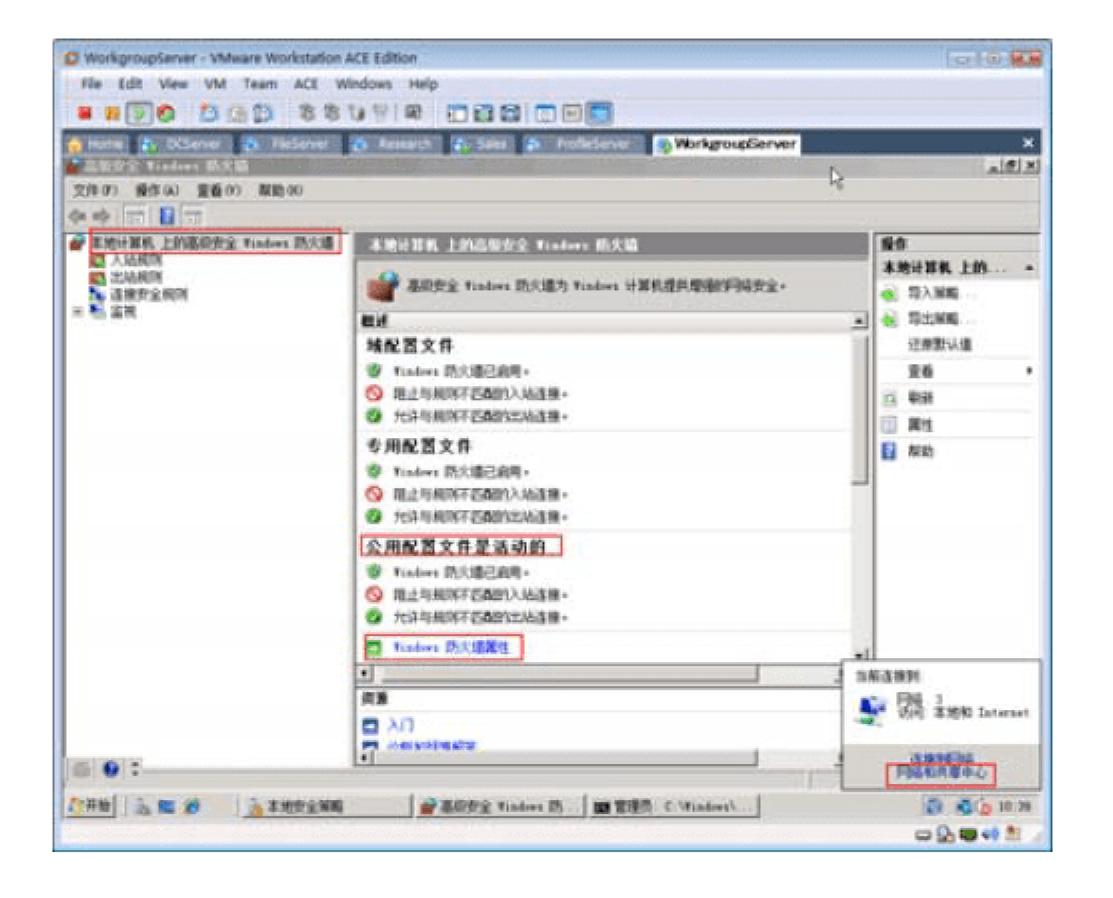


图 9-35　配置文件



图 9-36　“网络和共享中心”窗口

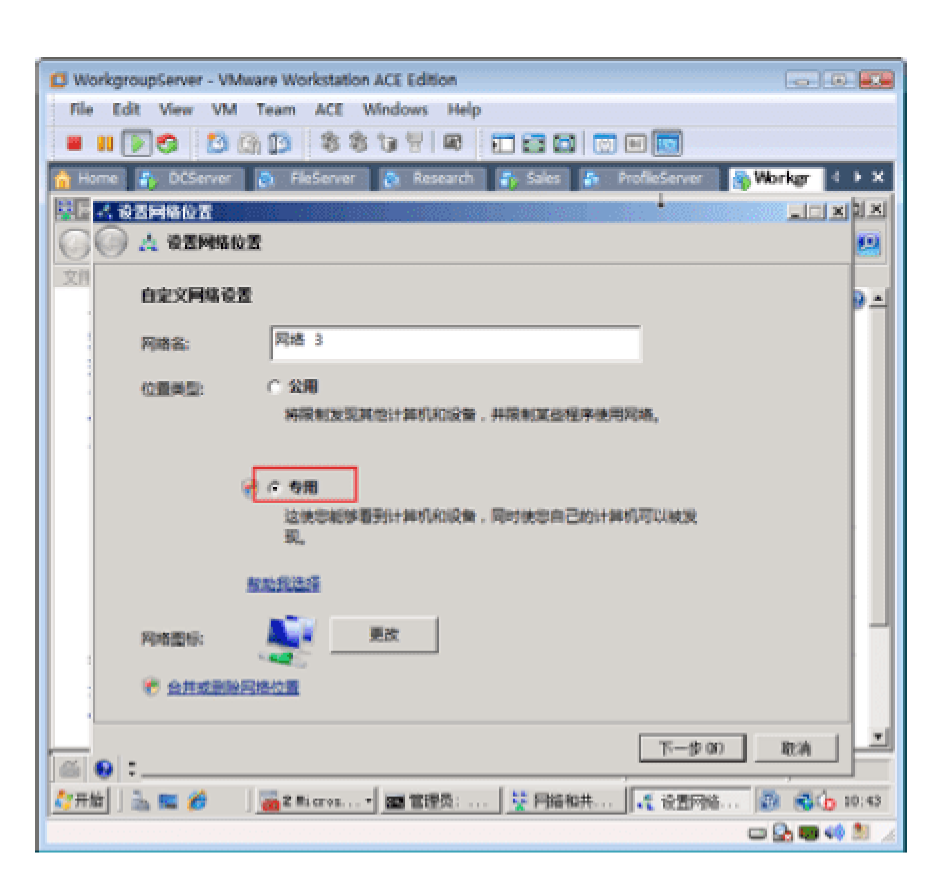
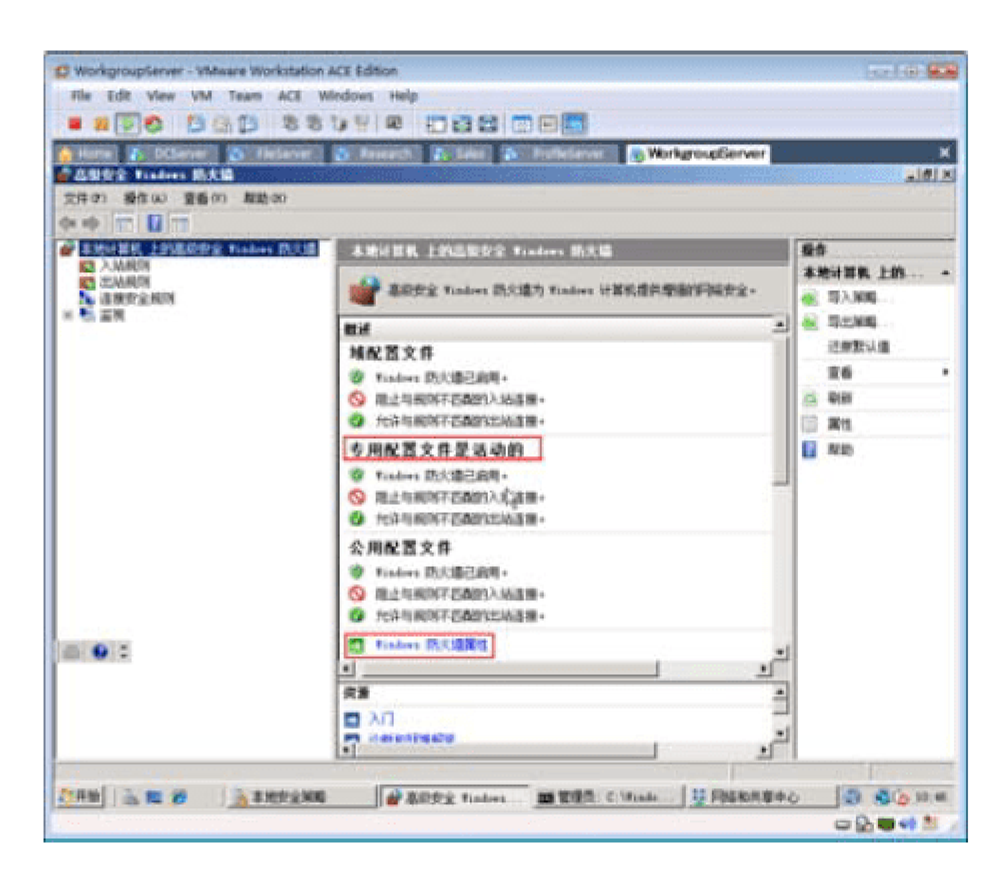


图 9-37　更改网络位置

⑥　如图 9-38 所示，再次打开“高级安全 Windows 防火墙”窗口，看到专用配置文件是活动的。

⑦　如图 9-39 所示，单击“Windows 防火墙属性”，在出现的 Windows 防火墙属性对话框中，切换到“专用配置文件”选项卡，防火墙状态为“启用”，入站连接默认“阻止”，出站连接默认“允许”。



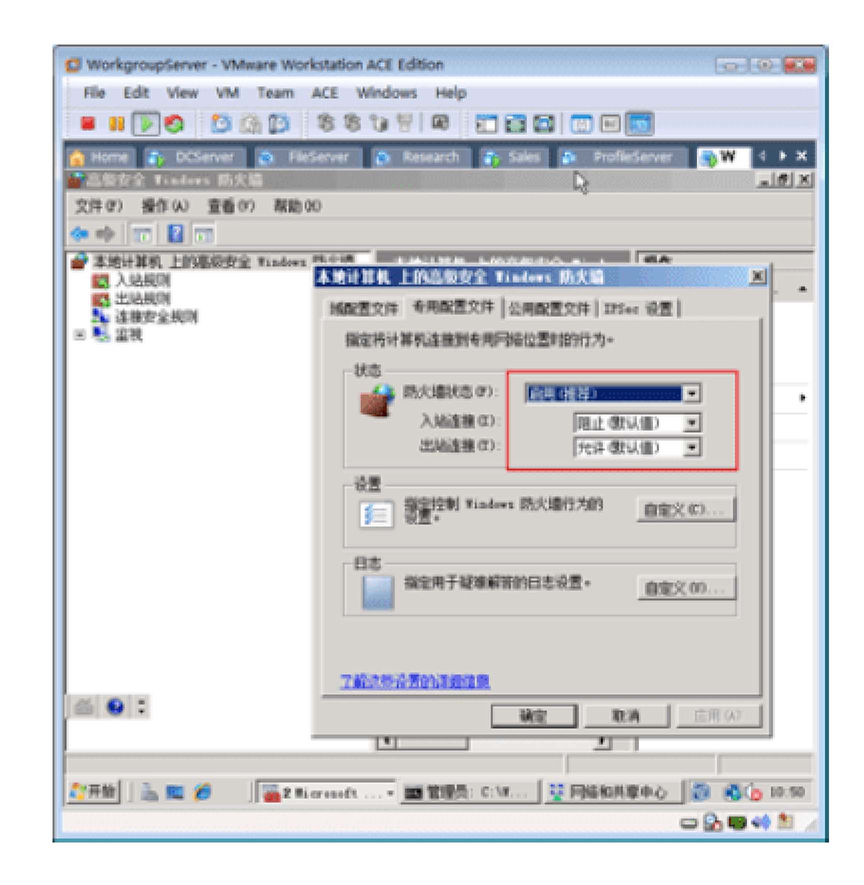


图 9-38 查看活动的配置文件　　　　图 9-39 配置 Windows 防火墙

⑧ 如图 9-40 所示，单击“入站筛选”选项，可以看到所有的预定义的入站规则，单击“按配置文件”选项，选择“按专用配置文件筛选”命令。

⑨ 如图 9-41 所示，现在看到的入站规则都是专用配置文件的规则，单击“已启用”选项，可以按启用与否排序。

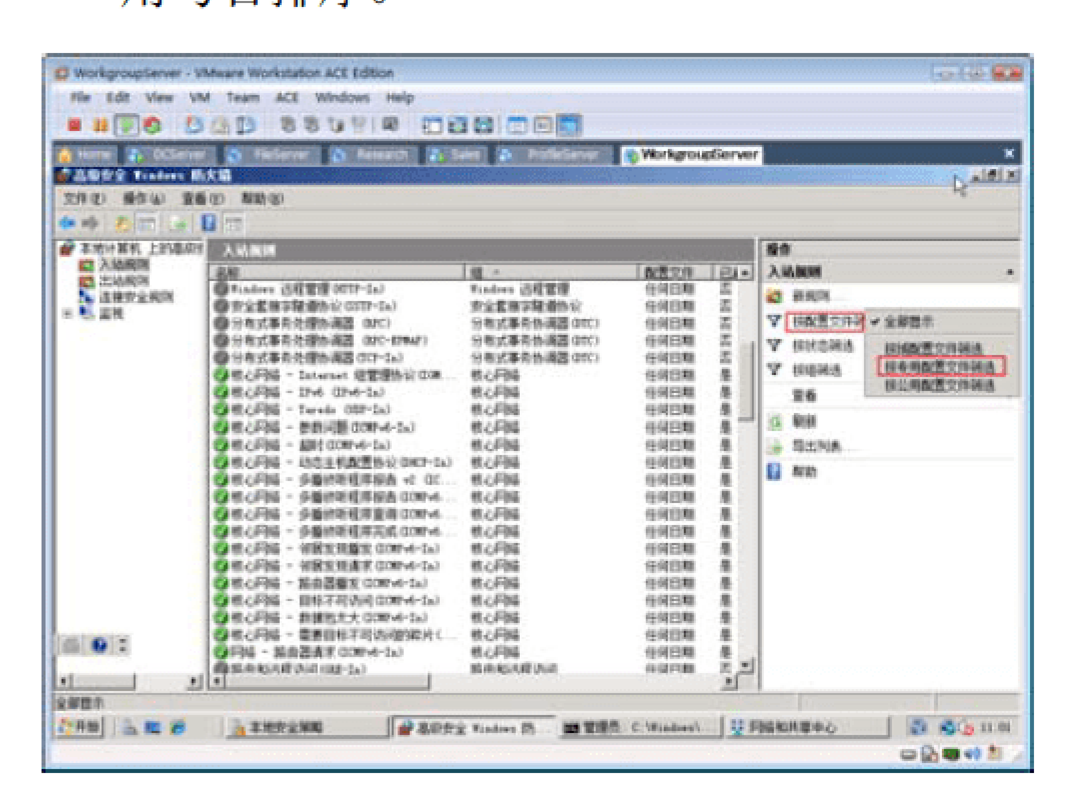


图 9-40 筛选规则

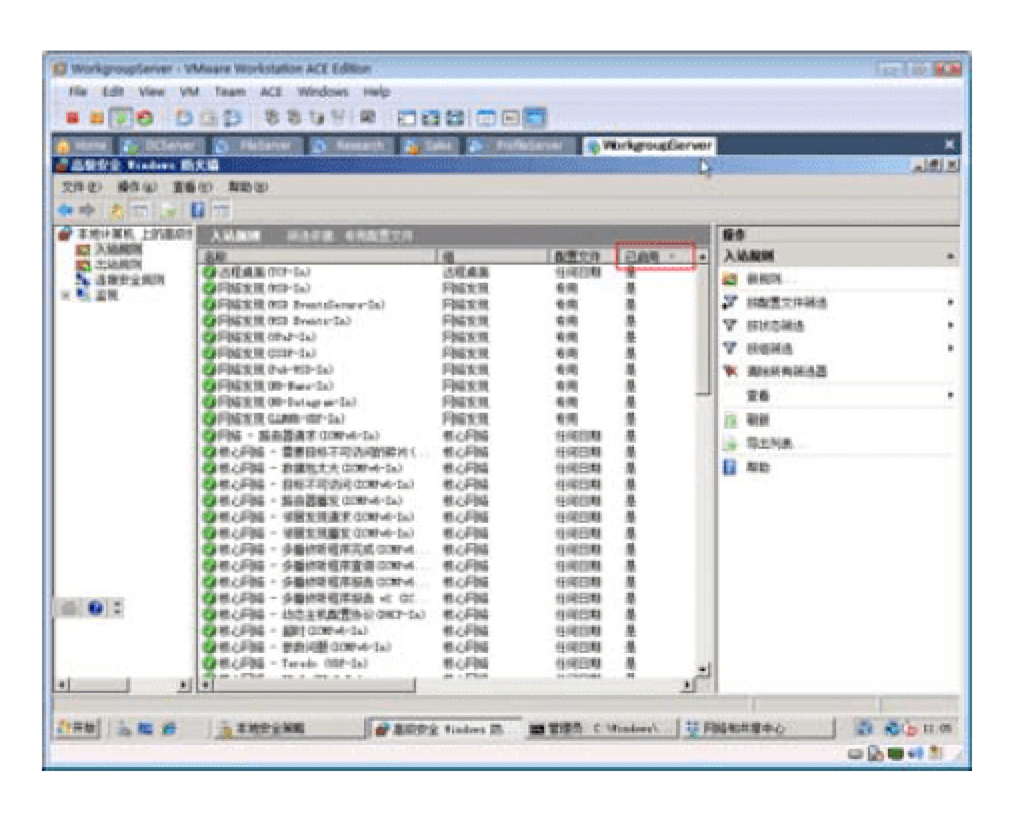


图 9-41 排序规则

⑩ 如图 9-42 所示，打开“网络和共享中心”窗口，启用“文件共享”、“打印机共享”、“网络发现”。

⑪ 如图 9-43 所示，再次查看防火墙规则、入站规则，打开了相应端口。

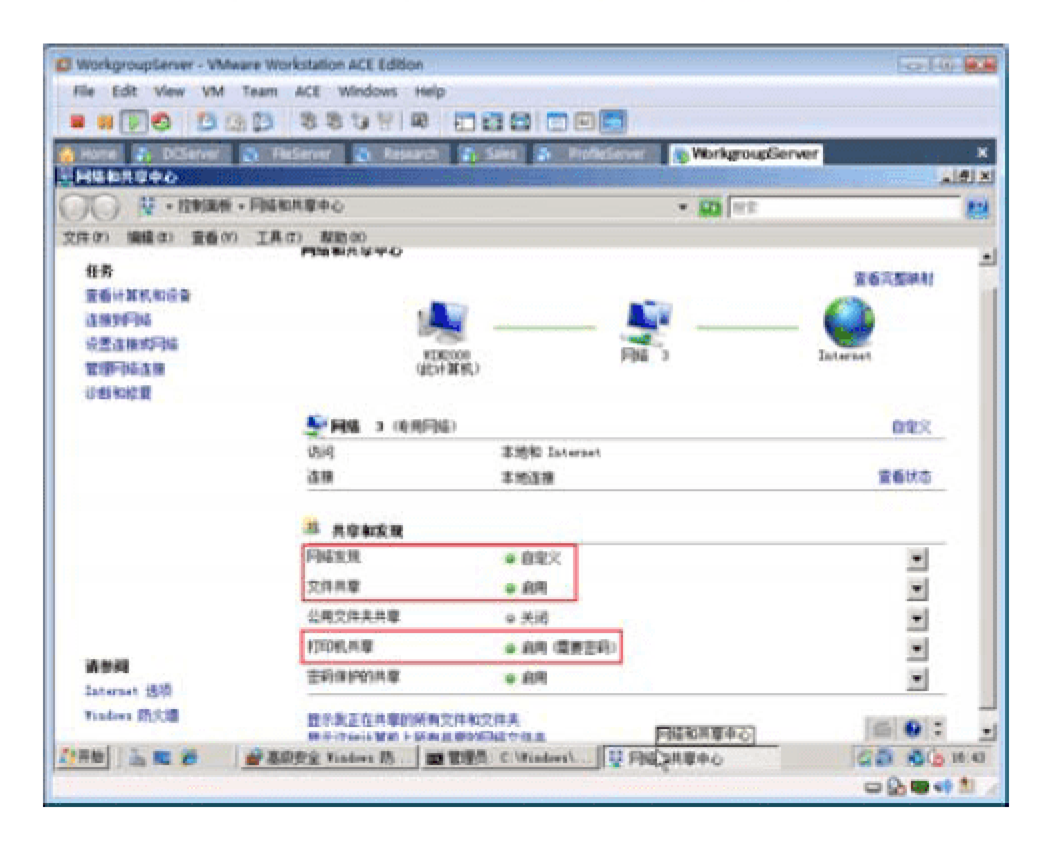


图 9-42 配置网络发现

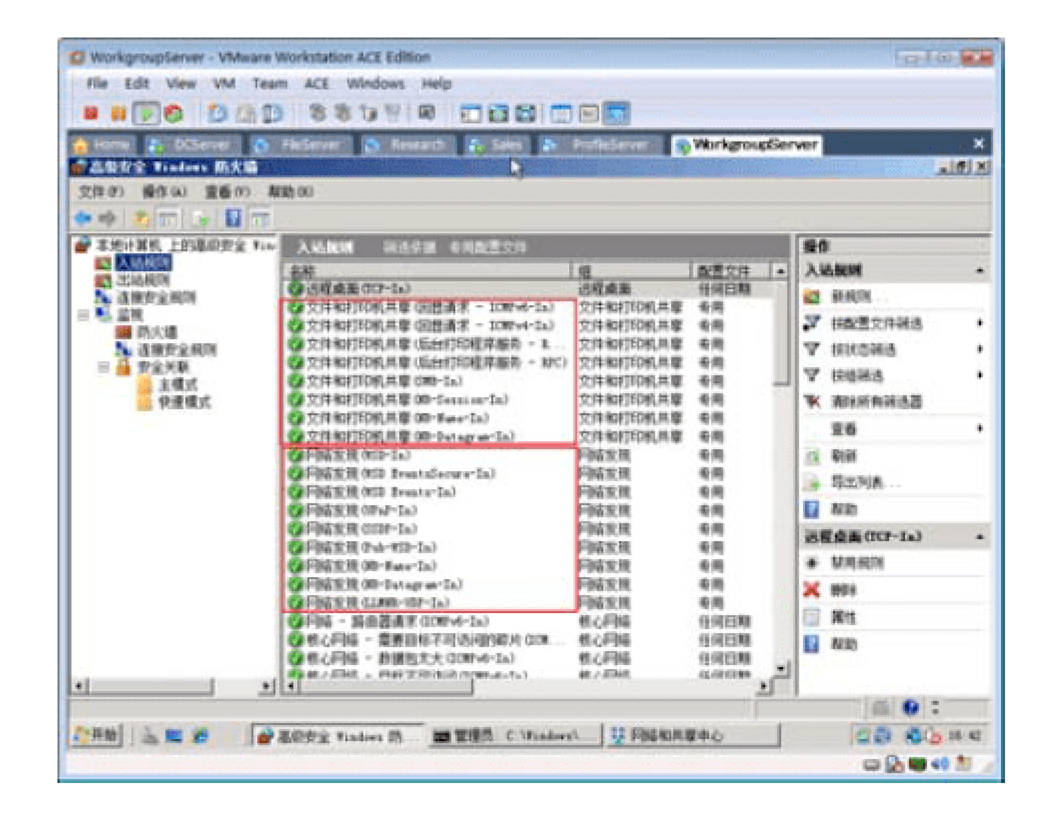


图 9-43 更改网络发现实质上是更改防火墙端口

9.6.4 示例：配置 Web 服务器网络安全

高级 Windows 防火墙不但能够控制进入计算机的数据流量，还能控制流出的流量。

1. 最大化 Web 服务器安全

如图 9-44 所示。

- 在 WorkgroupServer 上安装 IIS，配置 Web 站点。

■ 只允许目标端口是 80 的数据包进入 Web 服务器。
■ 只允许源端口是 80 的数据包从 Web 服务器出来

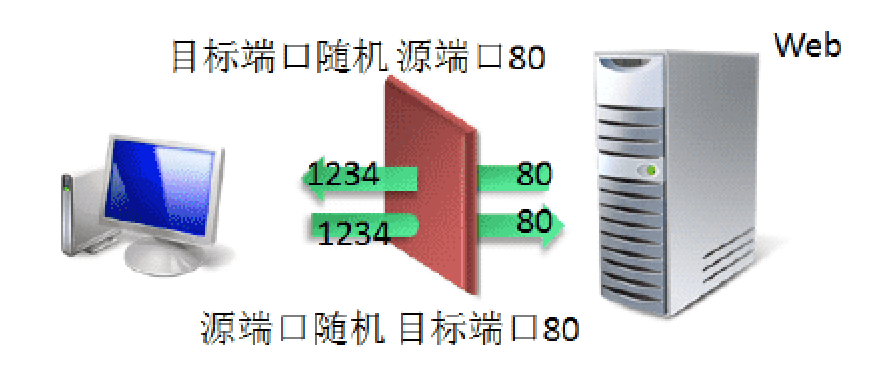


图 9-44 访问 Web 服务器流量

2. 实战环境

■ WorkgroupServer 是工作组中的计算机，安装了 Windows Server 2008 企业版。IP 地址是 10.7.10.125。
■ DCServer 是安装了 Windows Server 2008 的企业版。IP 地址是 10.7.10.12。

3. 步骤

① 如图 9-45 所示，打开服务器管理器，单击“添加角色”按钮。
② 如图 9-46 所示，在出现的“选择服务器角色”界面中，选中“Web 服务器”复选框，单击“下一步”按钮。

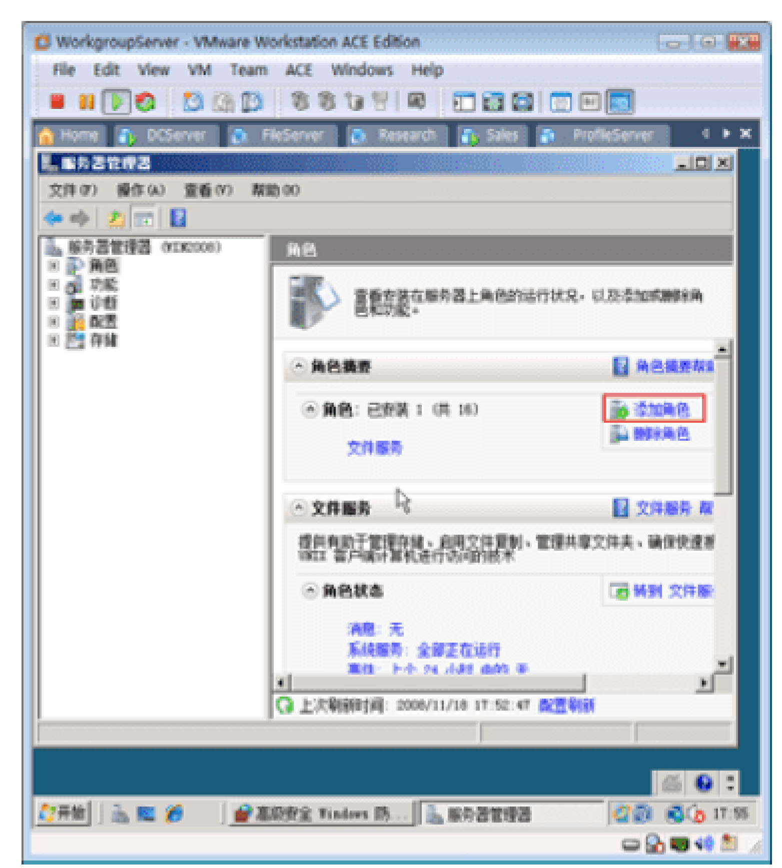


图 9-45 添加角色

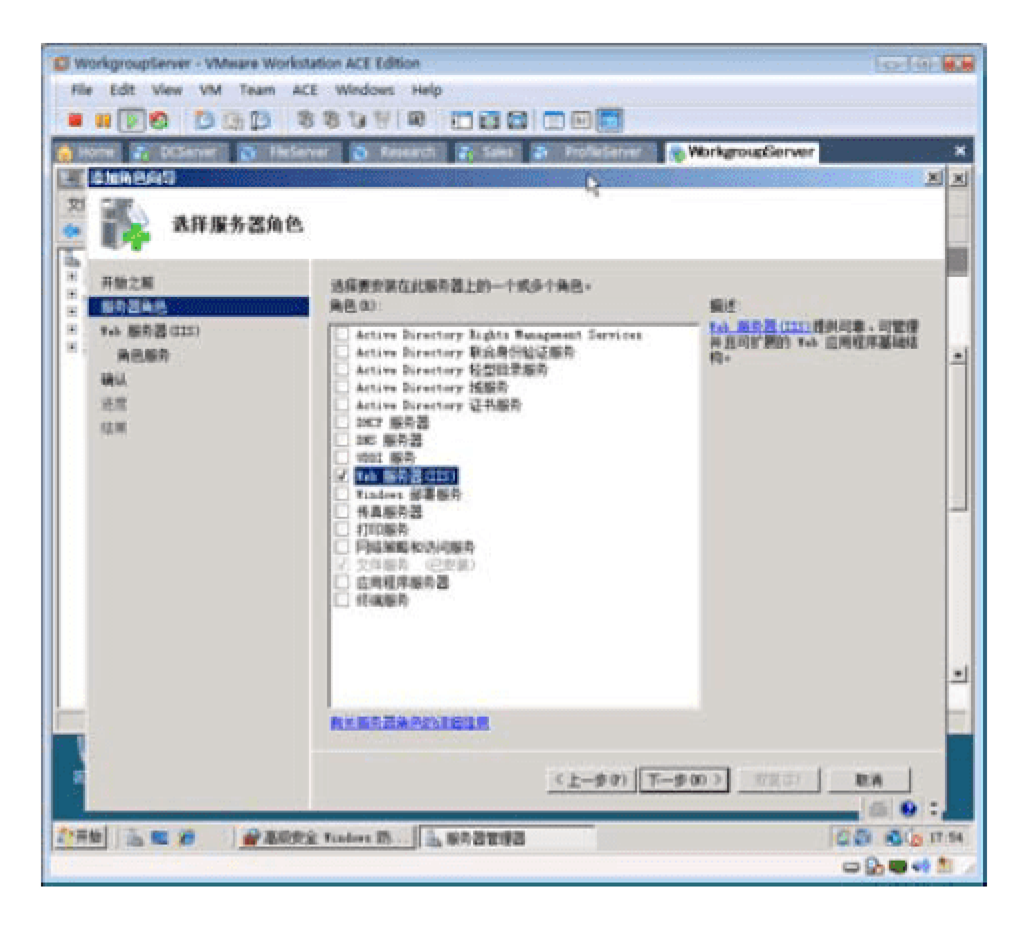


图 9-46 选择角色

③ 如图 9-47 所示，在弹出的对话框中，单击“添加必须的功能”。单击“下一步”按钮，完成安装。
④ 打开 http://www.baidu.com 网站，选择“文件”→“另存为”命令，将该网页保存到 C:\inetpub\wwwroot 目录下。
⑤ 选择“开始”→“程序”→“管理工具”→“Internet 信息服务(IIS)管理器”命令。
⑥ 如图 9-48 所示，单击“默认文档”图标。
⑦ 如图 9-49 所示，输入网页名称，单击“确定”按钮。
⑧ 如图 9-50 所示，单击 Default Web Site 选项后，单击“浏览*:80(http)”选项。
⑨ 如图 9-51 所示，可以打开本地网站的网页。
⑩ 如图 9-52 所示，打开“网络和共享中心”窗口，将位置更改为“公用网络”，如图 9-52 所示，

设置“共享和发现”。

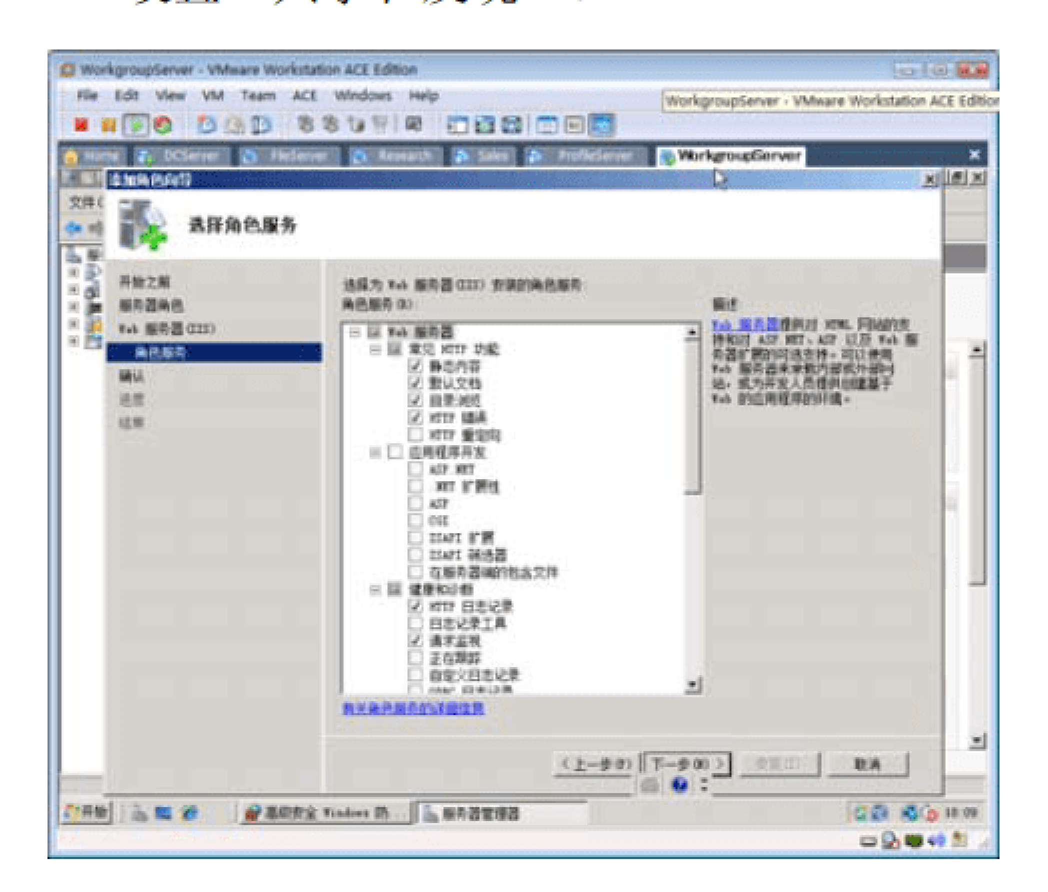


图 9-47　选择角色服务

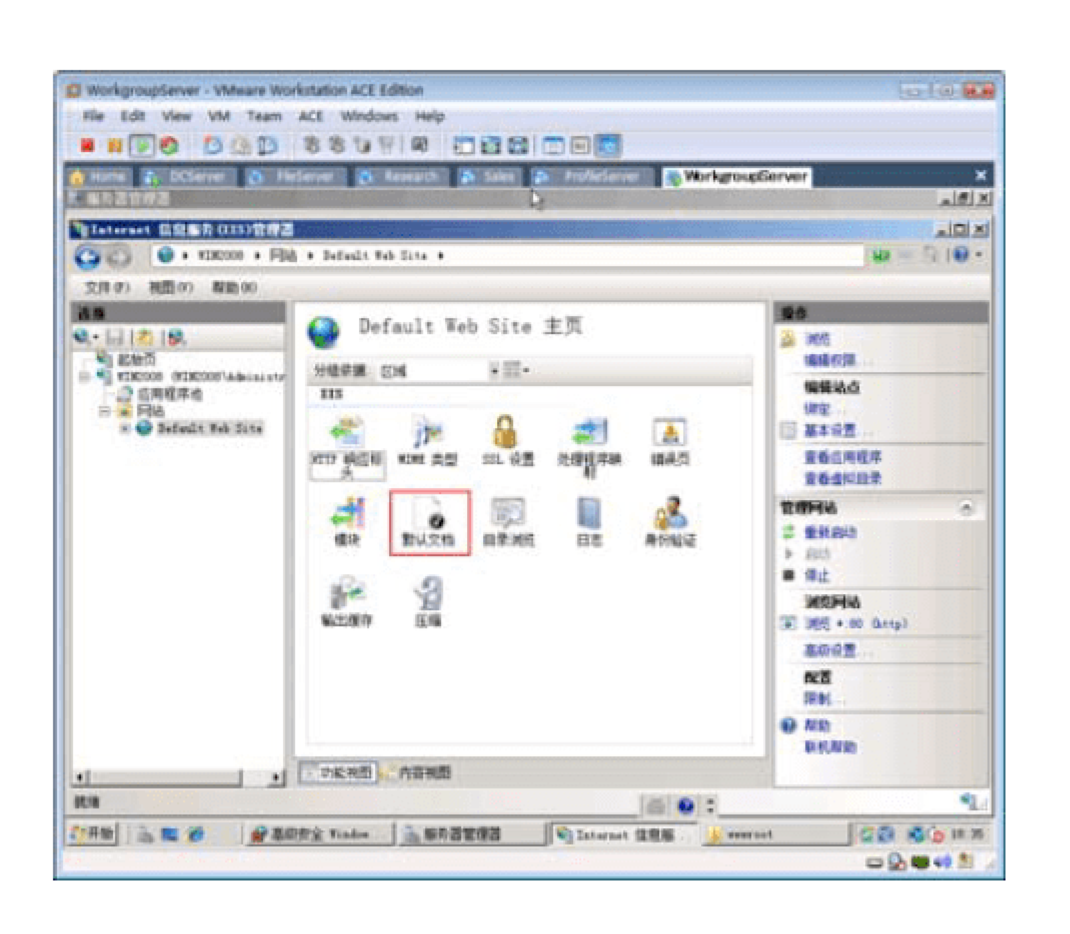


图 9-48　设置默认文档

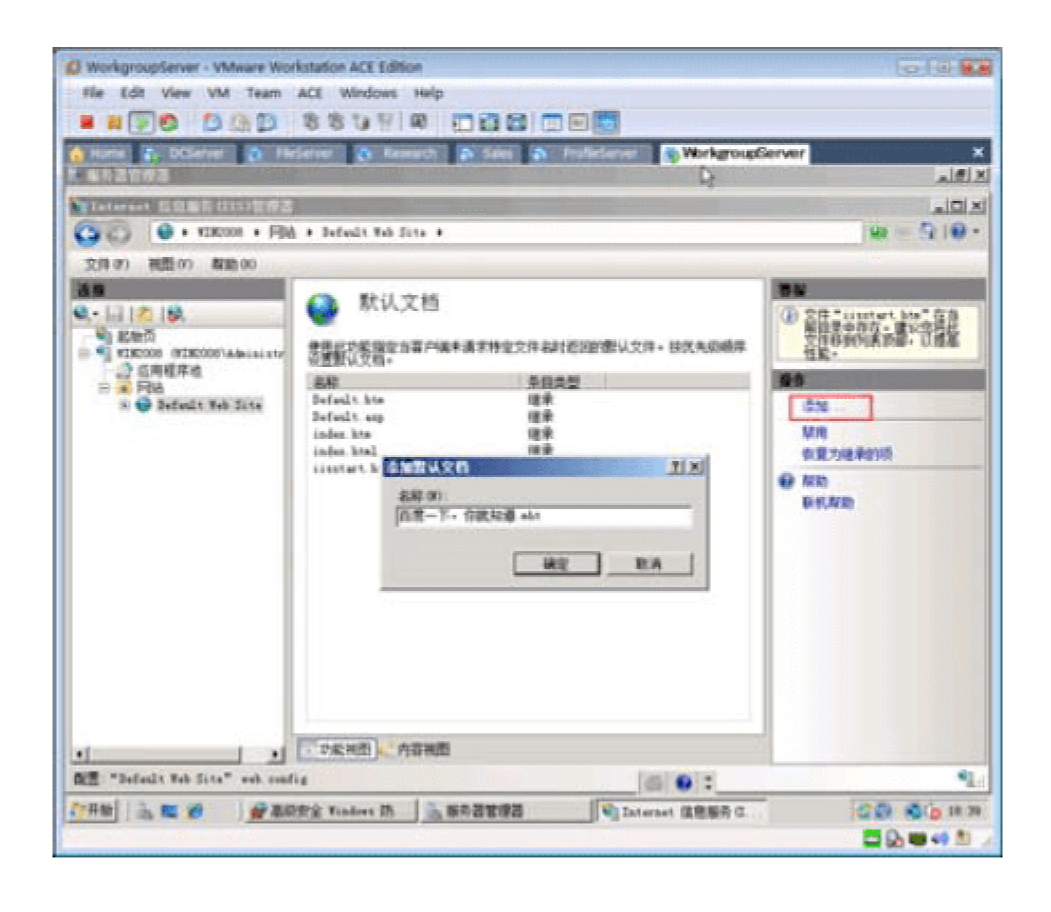


图 9-49　输入网页名称

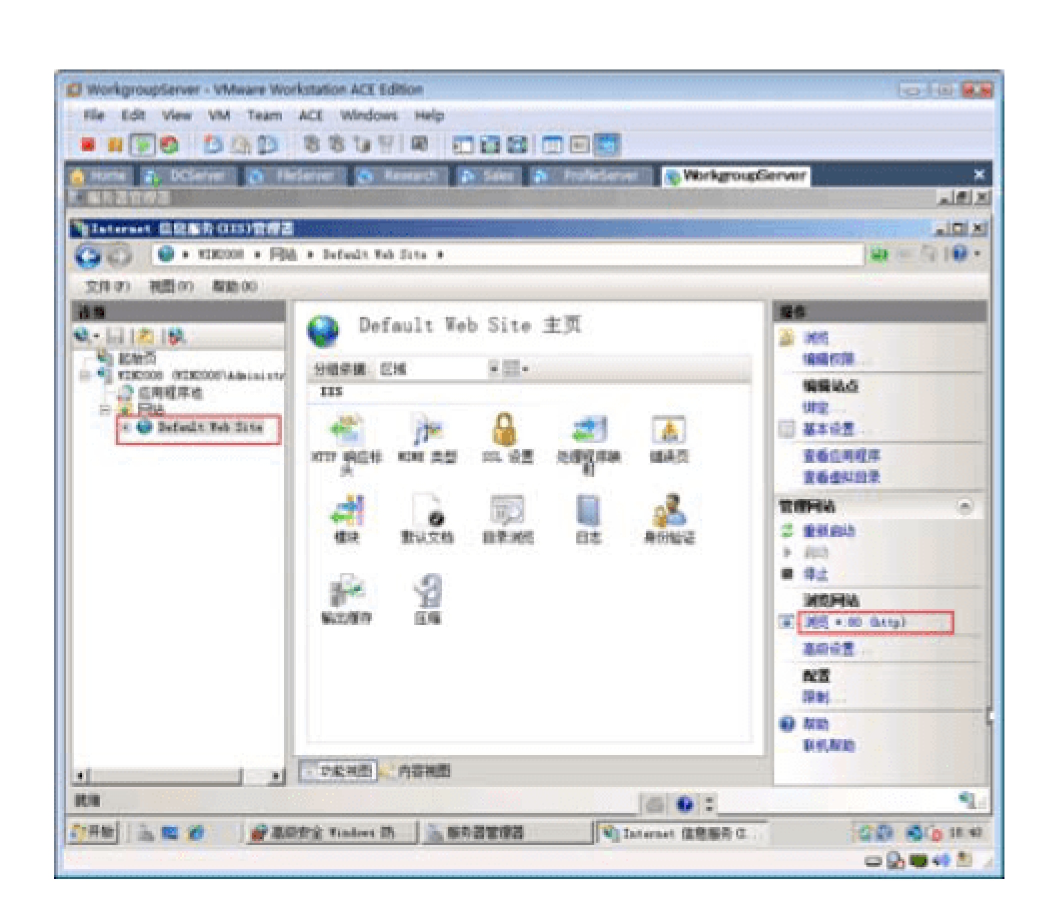


图 9-50　定位本地站点

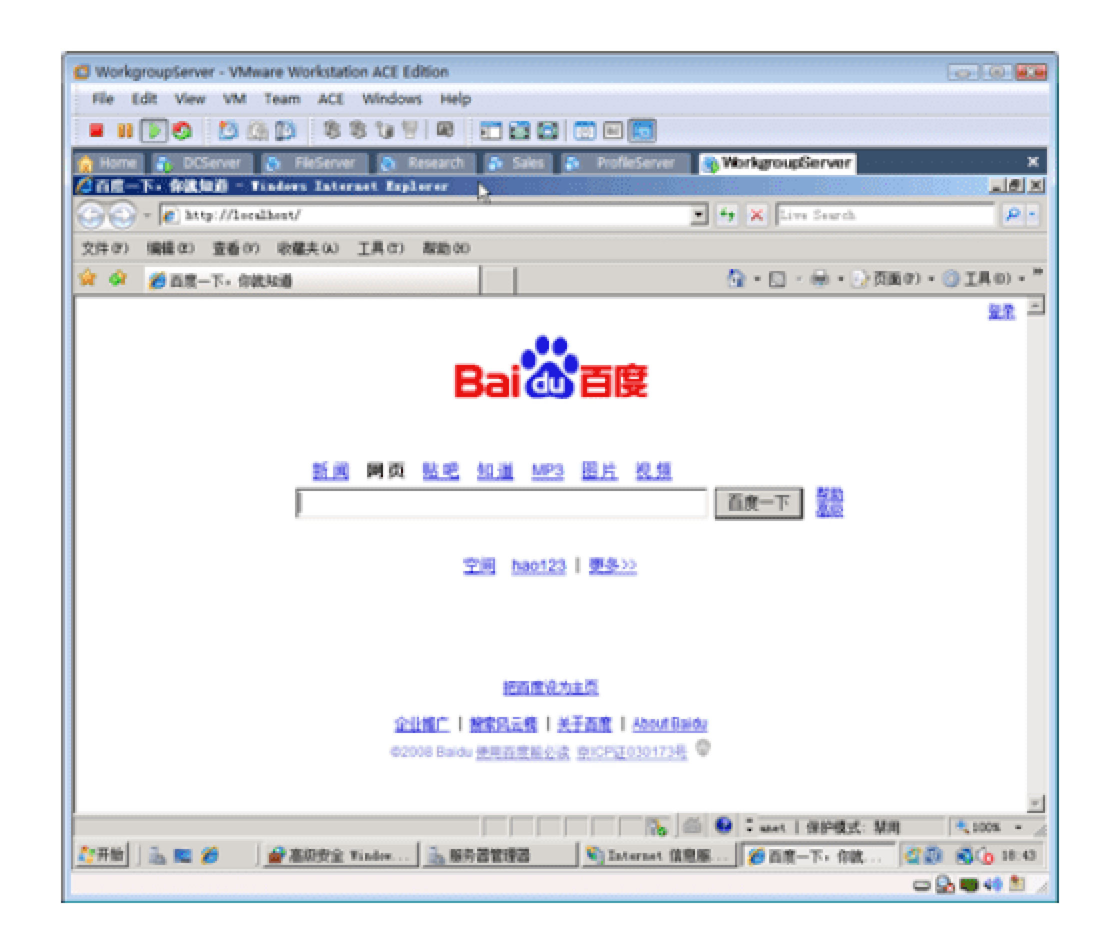


图 9-51　浏览网页



图 9-52　设置网络发现

⑪ 如图 9-53 所示，打开 Windows 防火墙属性，将公用配置文件出站连接默认设置成“阻止”。

⑫ 如图 9-54 所示，将公用配置文件其他的规则都禁用，只留下“万维网服务(HTTPS 流入量)”和“万维网服务(HTTP 流入量)”。

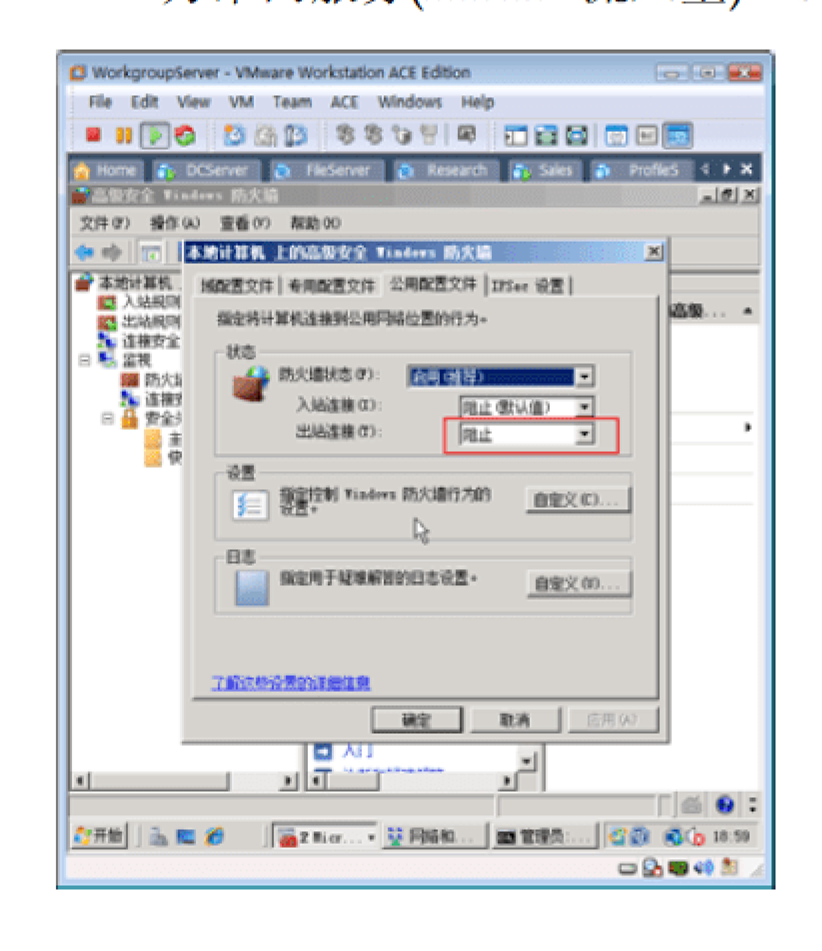


图 9-53 更改默认的出站规则

图 9-54 设置入站规则

⑬ 如图 9-55 所示，将出站连接的规则都禁用，右击“出站规则”，在弹出的快捷菜单中选择“新规则”命令。

⑭ 如图 9-56 所示，在出现的“规则类型”界面中，选中“端口”单选按钮，单击“下一步”按钮。

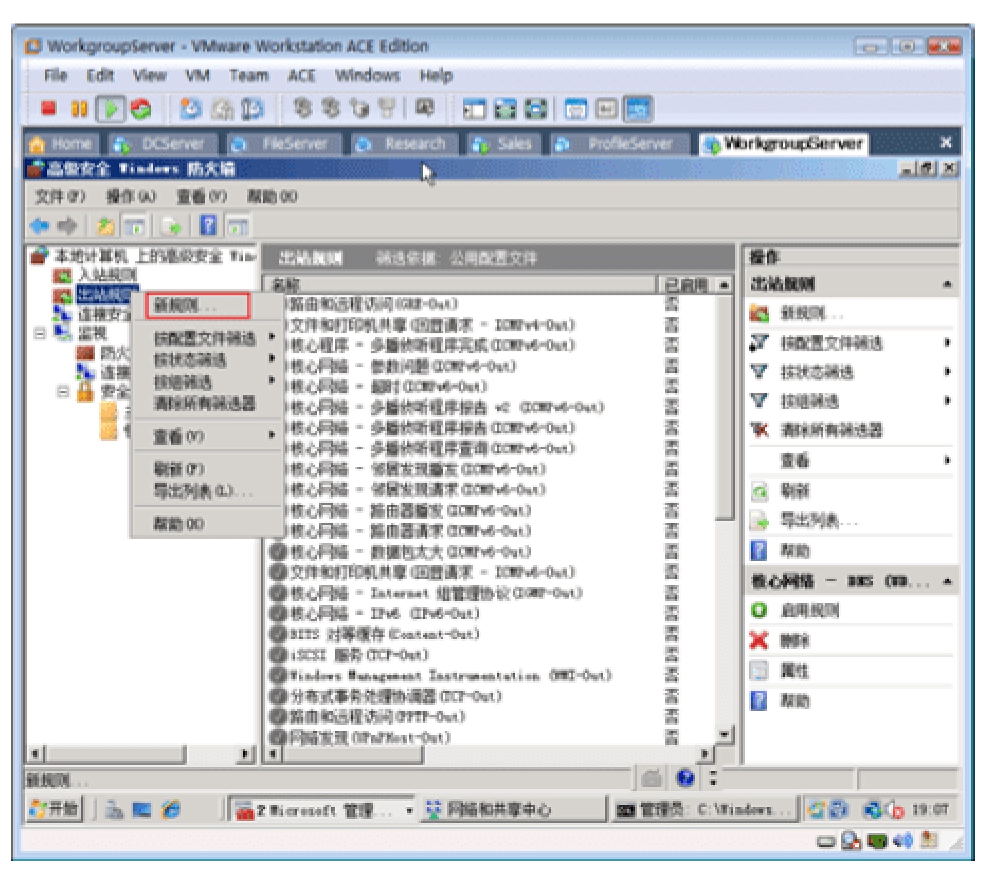


图 9-55 新建出站规则

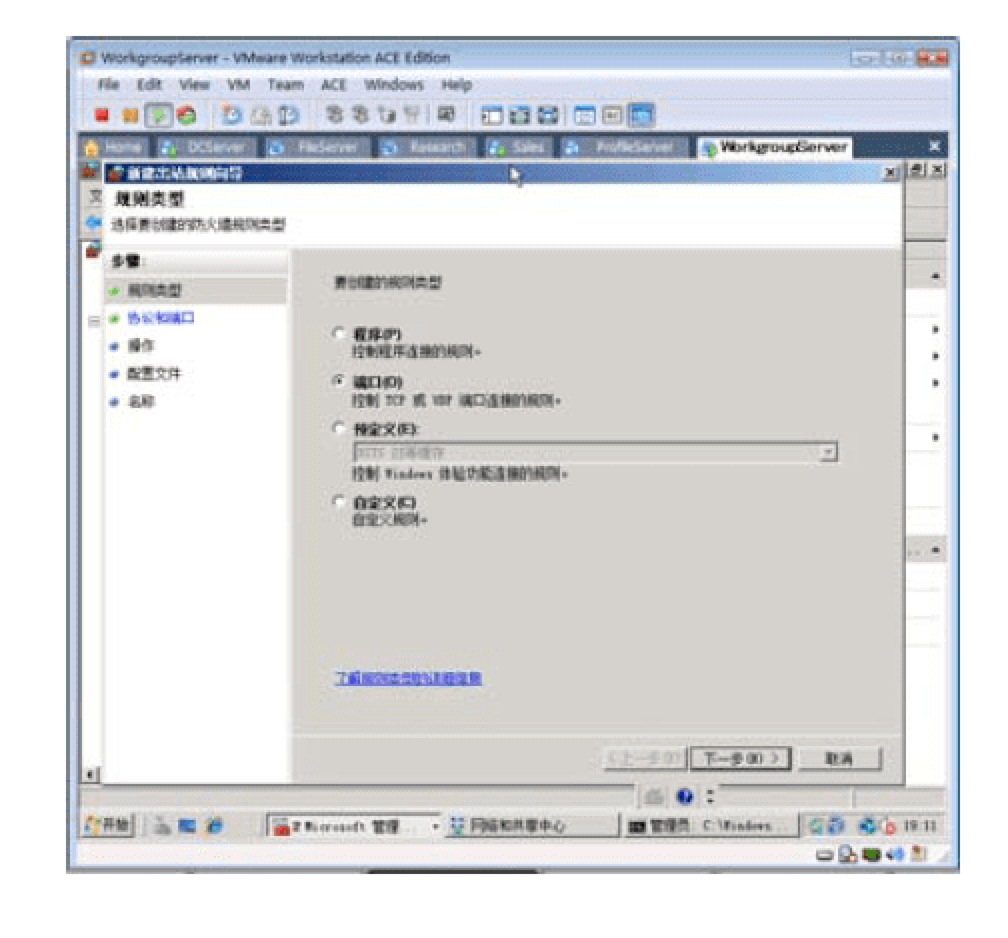


图 9-56 规则类型

⑮ 如图 9-57 所示，在出现的“协议和端口”界面中，将本地端口设置为 80，单击“下一步”按钮。

⑯ 如图 9-58 所示，在出现的“操作”界面中，选中“允许连接”单选按钮，单击“下一步”按钮。

⑰ 如图 9-59 所示，在出现的“配置文件”界面中，只选中“公用”复选框，单击“下一步”按钮。

⑱ 如图 9-60 所示，在出现的“名称”对话框中，输入规则名称，单击“下一步”按钮，完成出站规则创建。

⑲ 如图 9-61 所示，测试到 DCServer 的访问，ping 10.7.10.12，出现“一般故障”的提示。这说明已经控制了出站流量。

⑳ 如图 9-62 所示，在 DCServer 上，打开 IE 浏览器，输入 http://10.7.10.125，按 Enter 键。此时，

发现能够访问其站点。

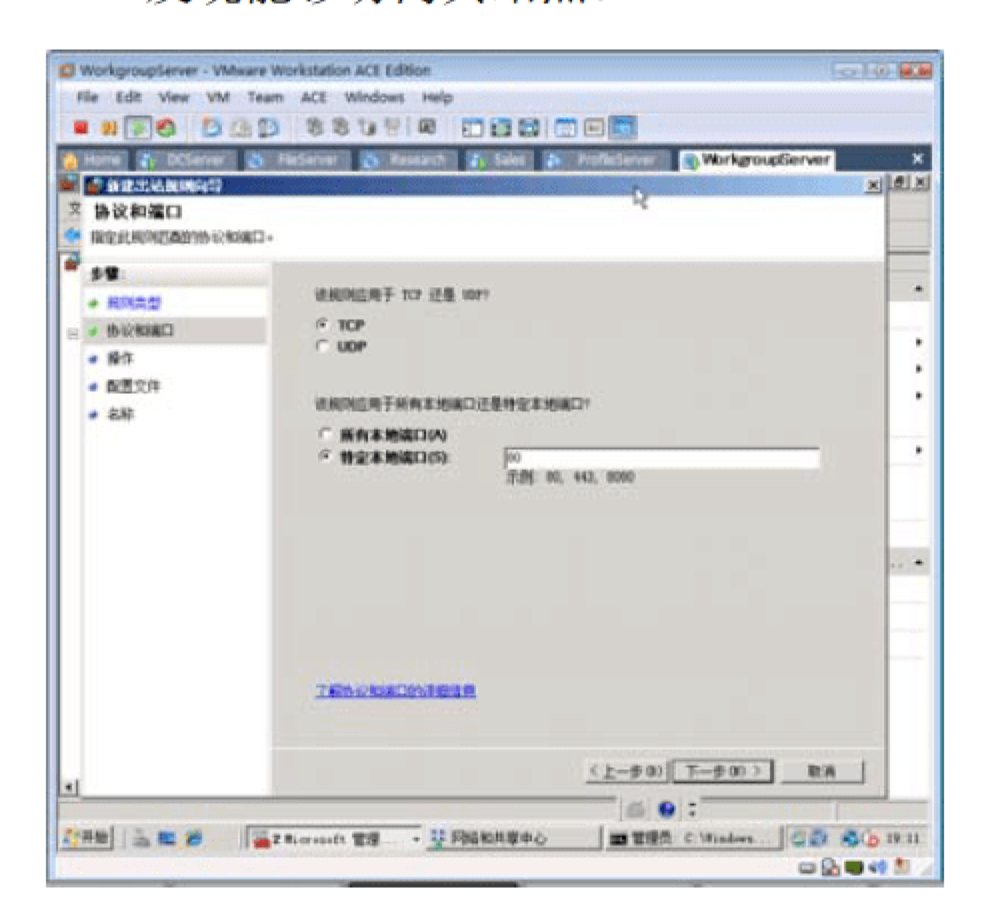


图 9-57 指定协议和端口

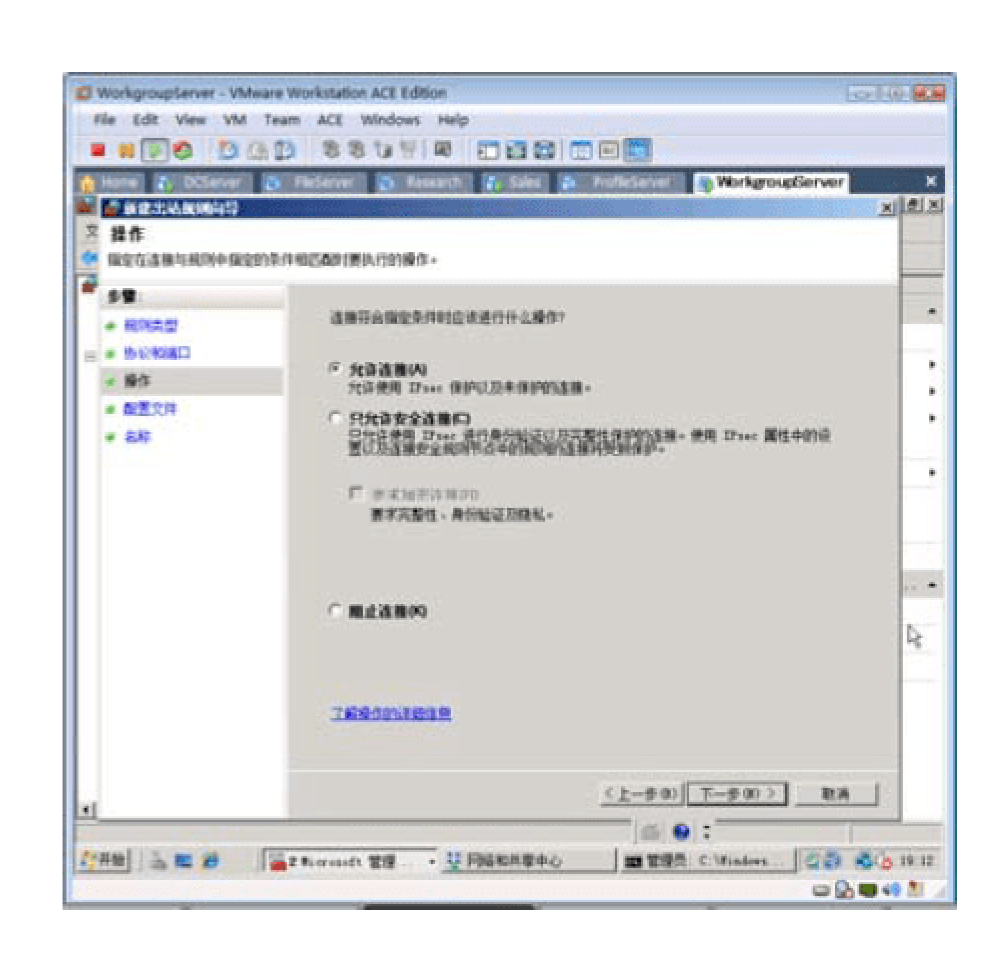


图 9-58 指定操作

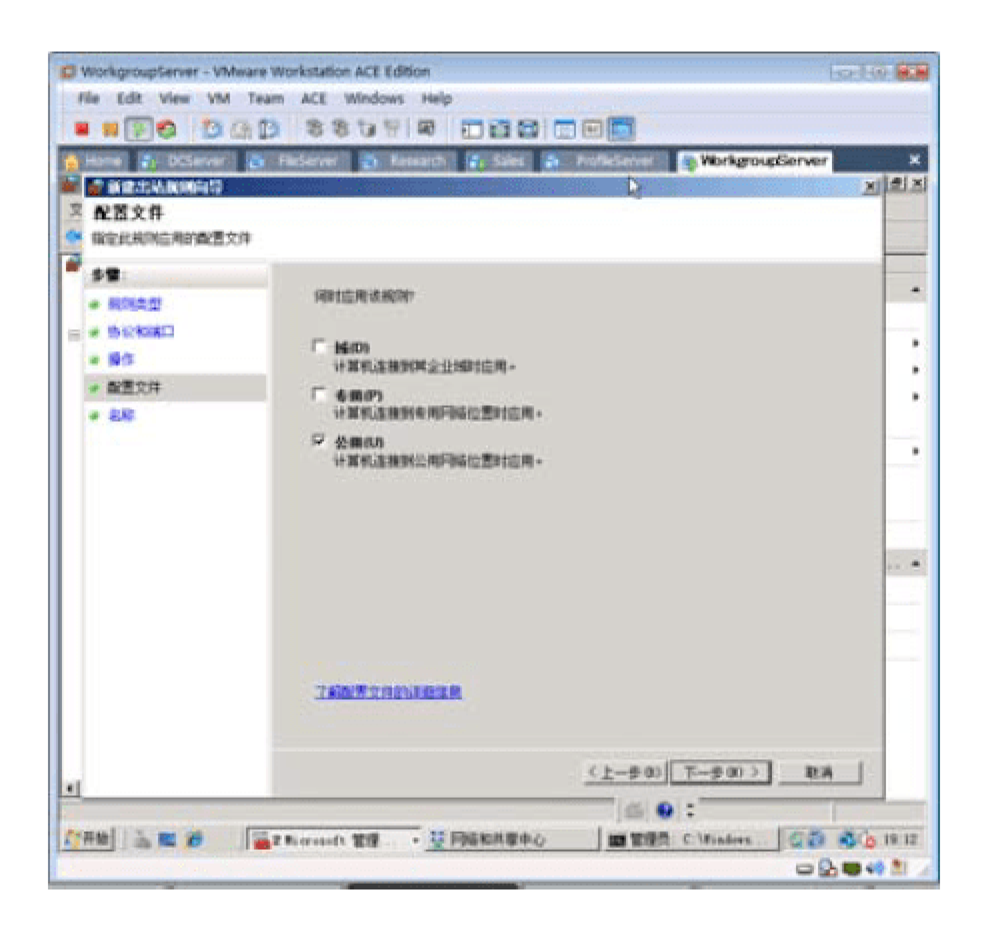


图 9-59 指定配置文件

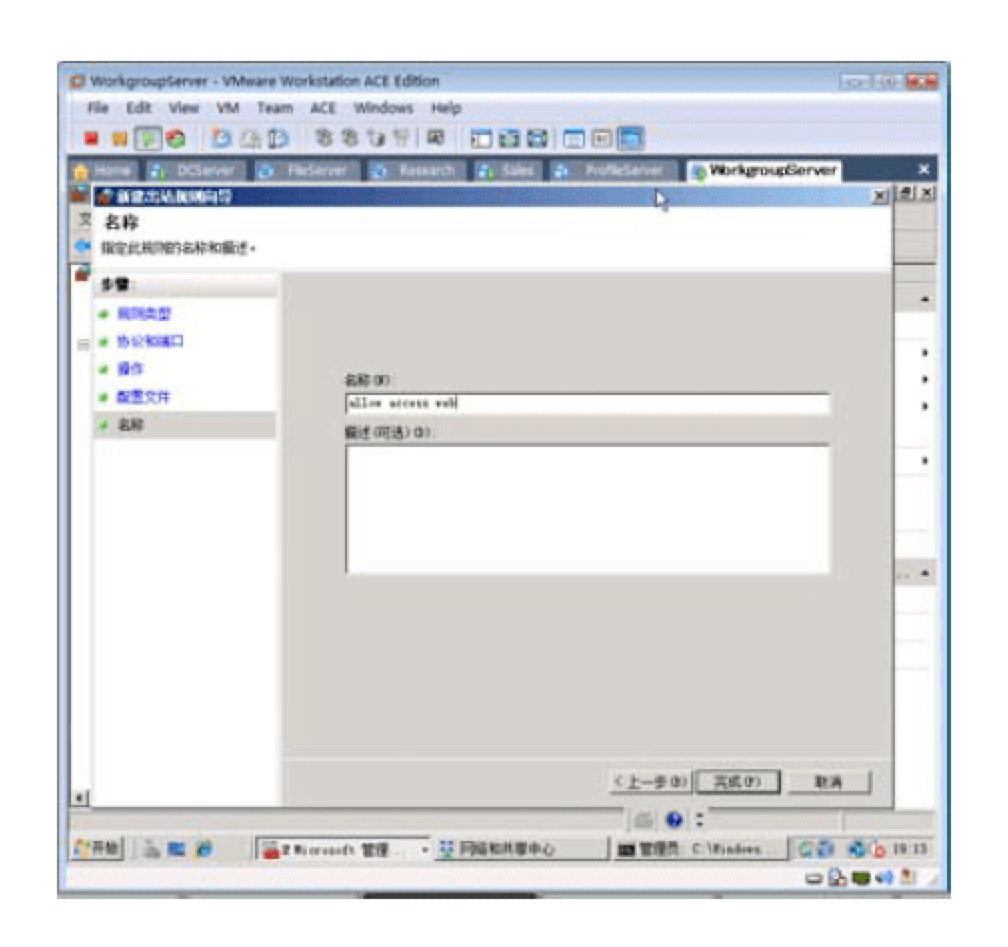


图 9-60 指定规则名称

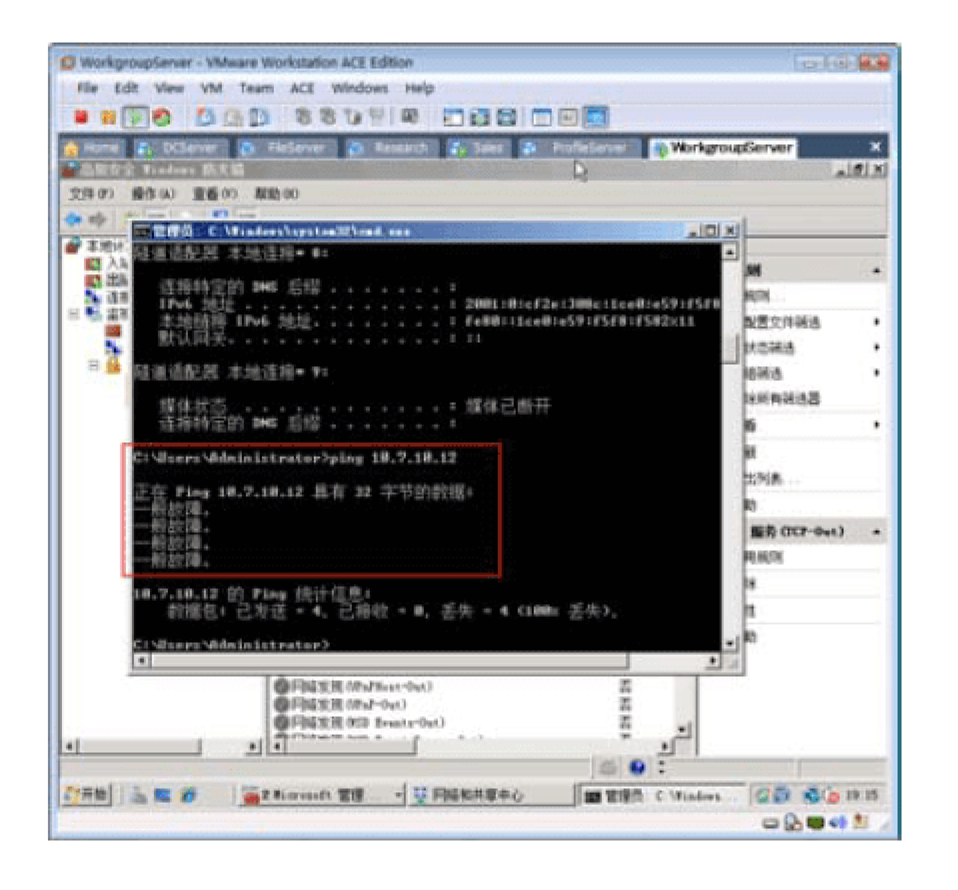


图 9-61 测试规则

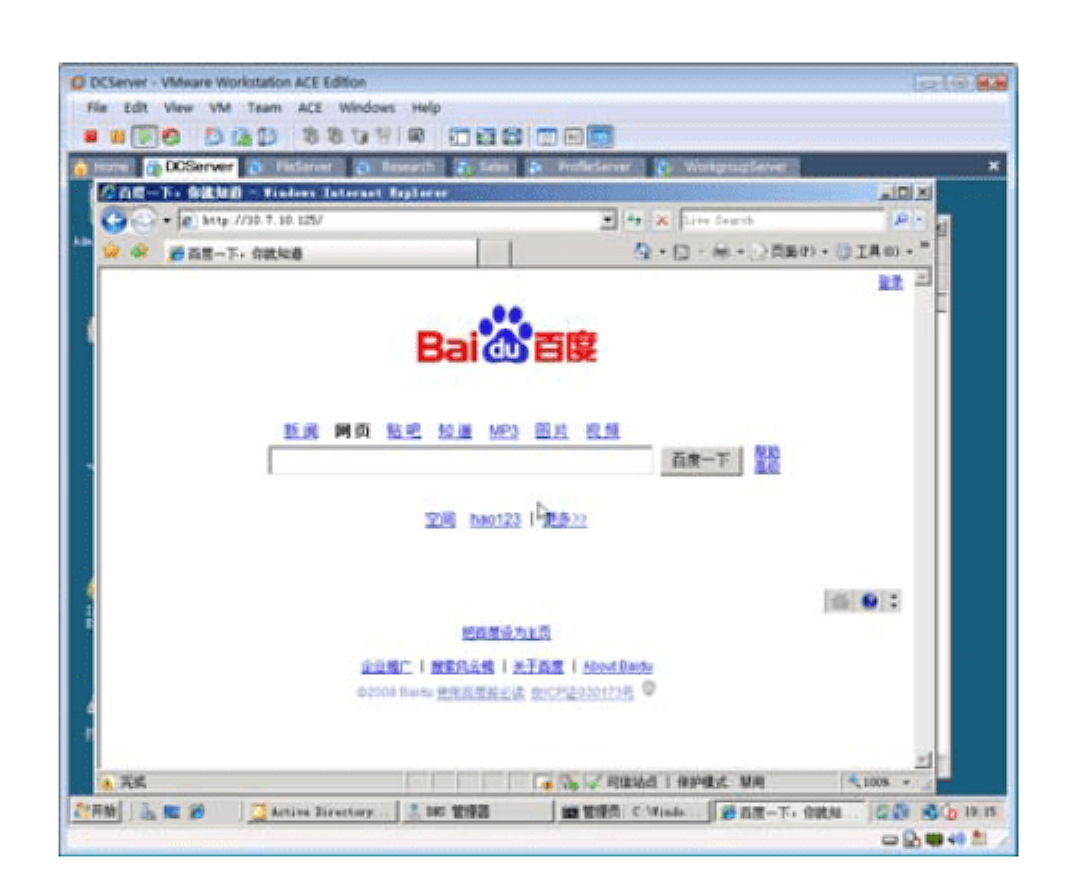


图 9-62 测试站点

㉑ 如图 9-63 所示，Ping 10.7.10.125，发现不通。

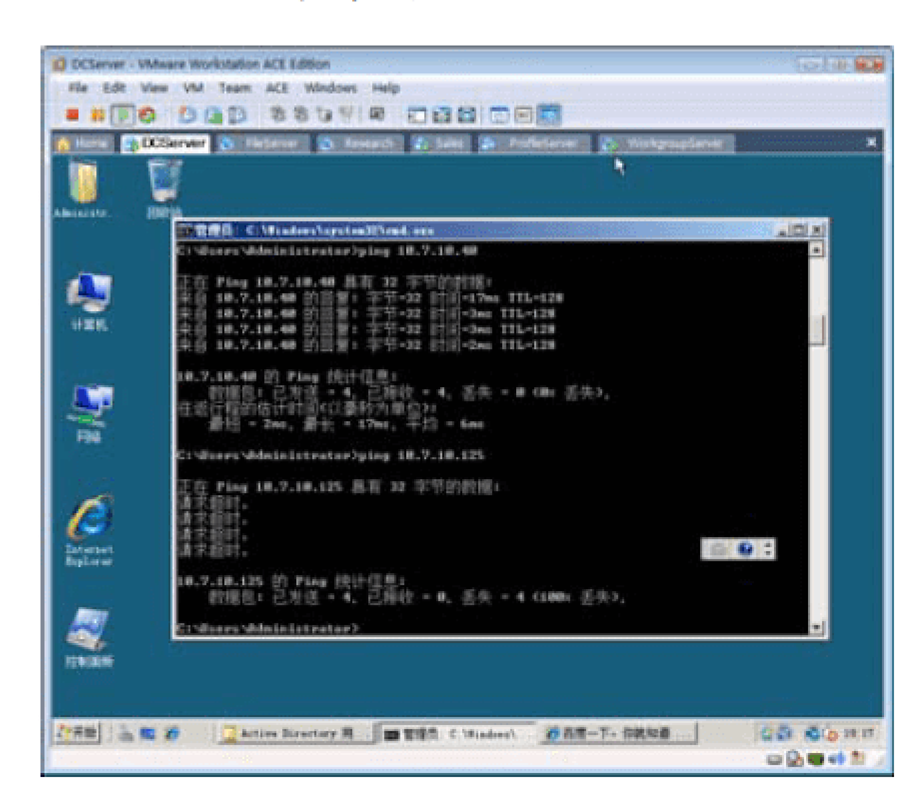


图 9-63　测试网络层

9.6.5　示例：配置加密通信

高级 Windows 防火墙除了能够允许或拒绝某些通信外，还支持加密通信。要想实现加密通信，需要配置连接安全规则。

1. 要求

服务器 Research 远程桌面，只允许 Sales 计算机和 WorkgroupServer 计算机访问。

要求到 Research 计算机远程桌面通信实现加密。

在域中的计算机可以使用 Kerberos 来验证对方计算机的身份。

工作组中的计算机使用共享密钥验证对方计算机的身份。

2. 实战环境

如图 9-64 所示。

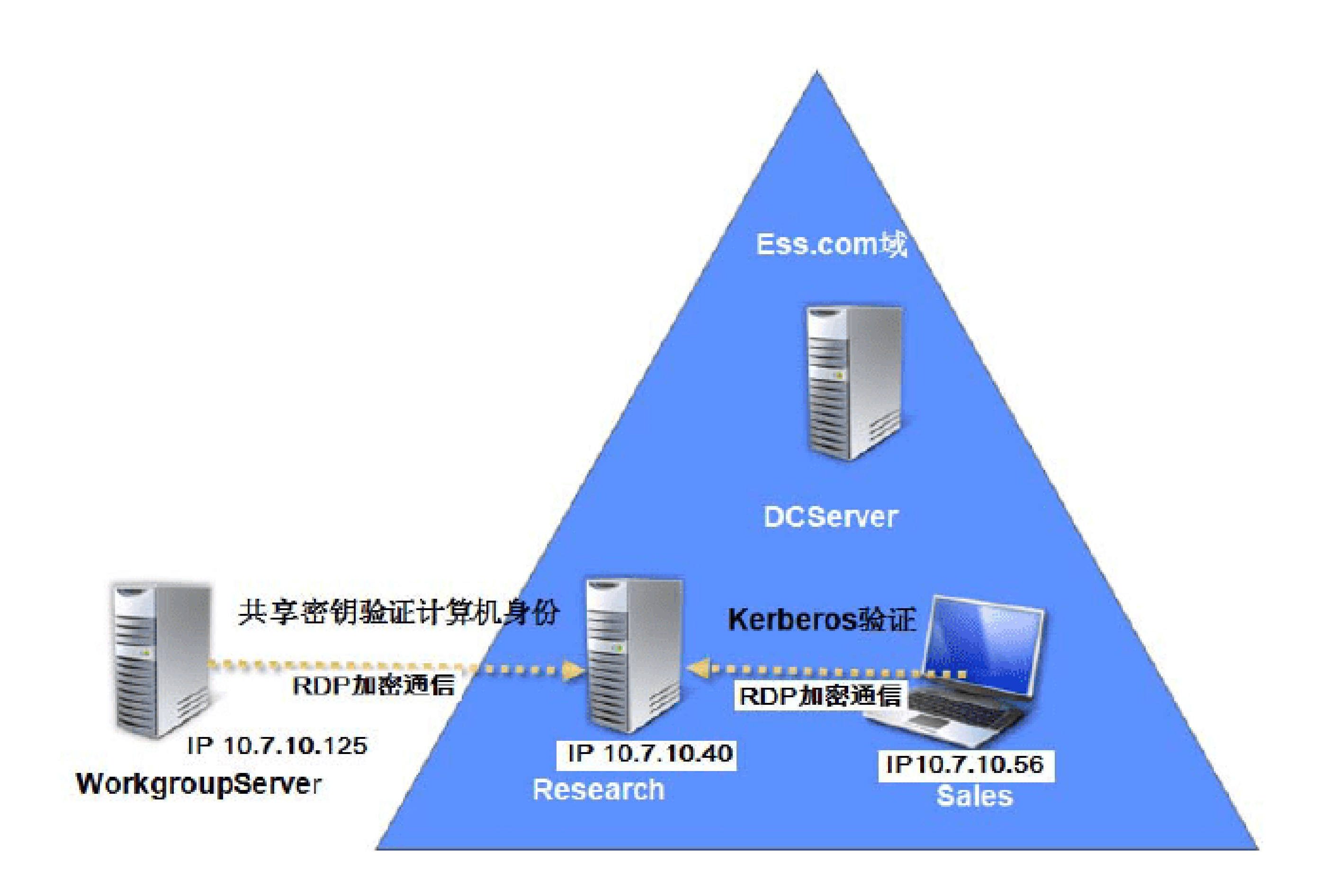


图 9-64　实战环境

DCServer 是 Ess.com 域中的域控制器。

Sales 是 Ess.com 域中的成员，Vista 操作系统，IP 地址 10.7.10.56。

Research 是 Ess.com 域中的计算机，IP 地址为 10.7.10.40。

WorkgroupServer 是工作组中的计算机，IP 地址为 10.7.10.125。

3. 步骤

① 在 Research 服务器上，以域管理员身份登录。

② 如图 9-65 所示，打开“控制面板”→“系统”，单击“远程设置”，选择“允许运行任意版本远程桌面的计算机连接”单选按钮，单击“确定”按钮。

③ 选择“开始”→“运行”命令，输入 wf.msc，打开高级 Windows 防火墙。

④ 如图 9-66 所示，可以看到当前活动的配置文件是域配置文件。查看入站规则，单击“按配置文件筛选”按钮，选择“按域配置文件筛选”选项。

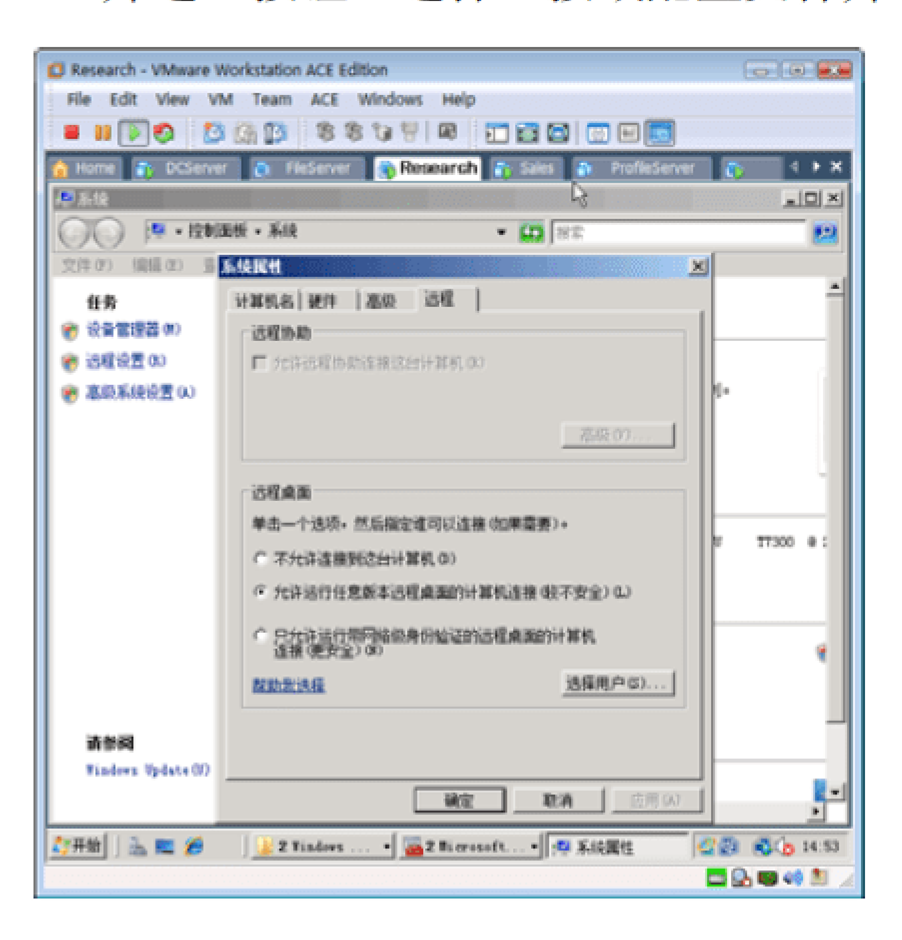


图 9-65　启用远程桌面

图 9-66　筛选规则

⑤ 如图 9-67 所示，双击入站规则“远程桌面(TCP-In)”，在“常规”选项卡中，选中“只允许安全连接”单选按钮，选中“要求加密”复选框。

⑥ 如图 9-68 所示，在“作用域”选项卡中，远程地址选择“下列 IP 地址”，单击“添加”按钮。

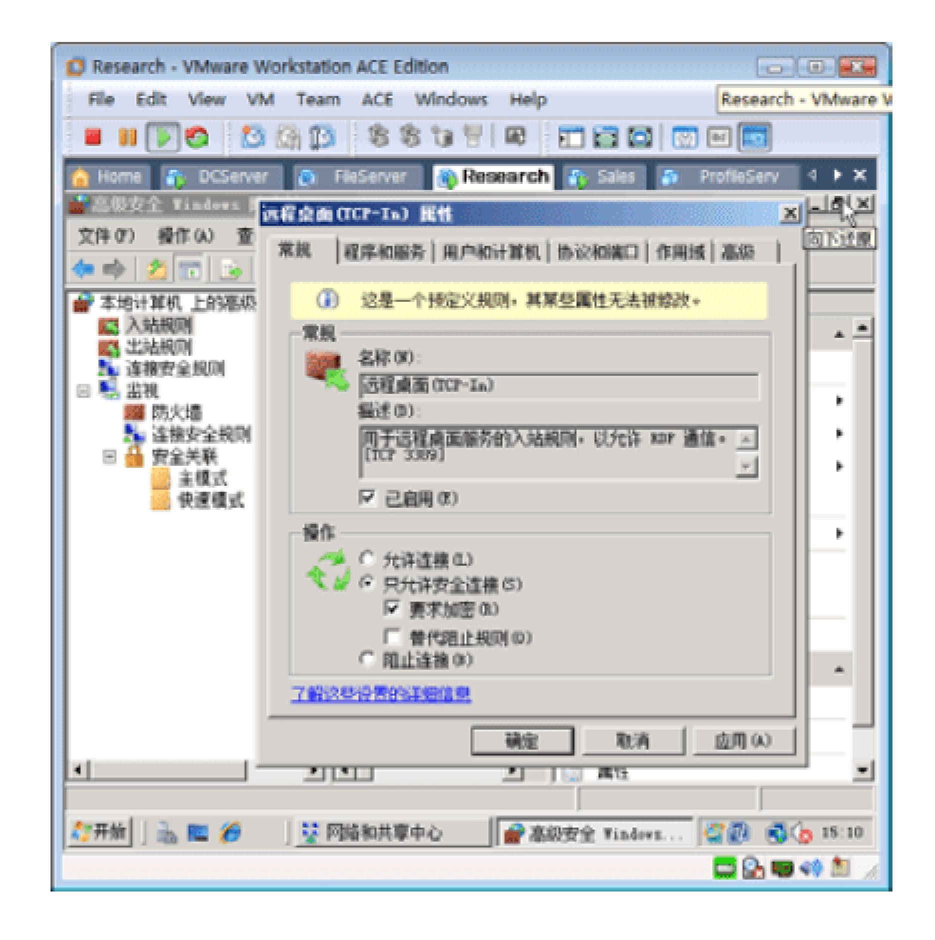


图 9-67　允许安全通信

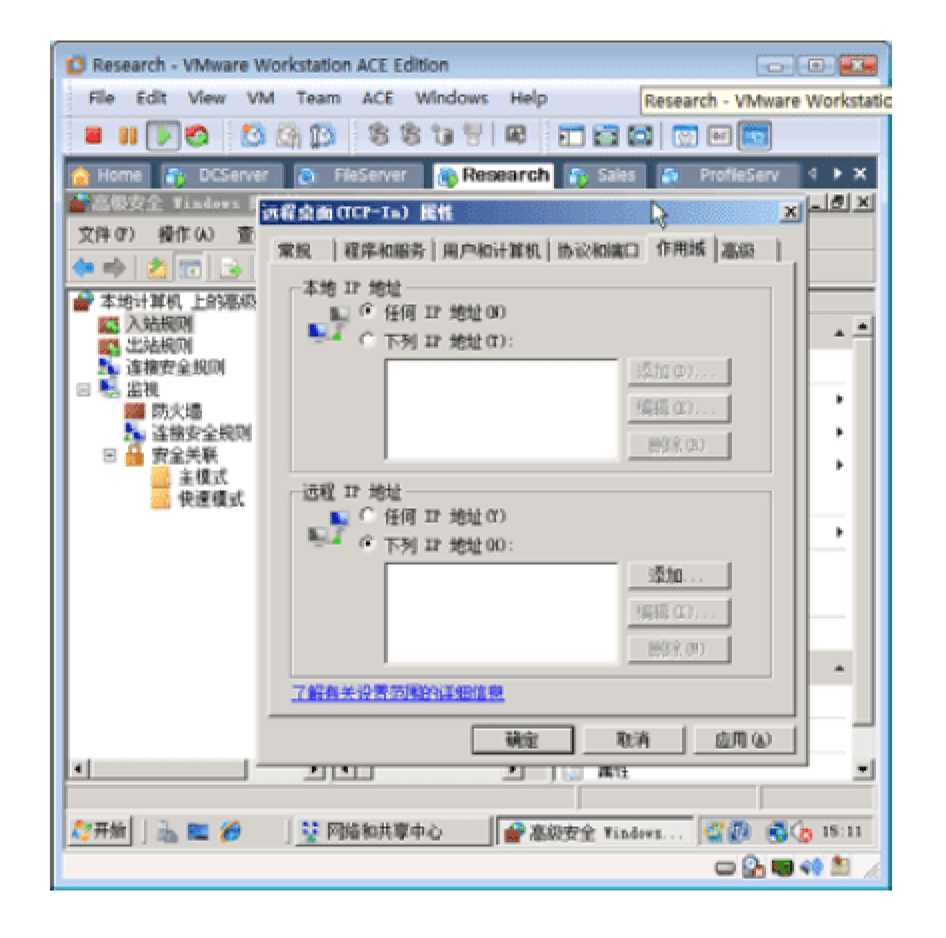


图 9-68　指定作用域

⑦ 如图 9-69 所示，添加 10.7.10.125 和 10.7.10.56 两个地址，单击“确定”按钮。

⑧ 如图 9-70 所示，右击“连接安全规则”选项，在弹出的快捷菜单中选择“新规则”命令。

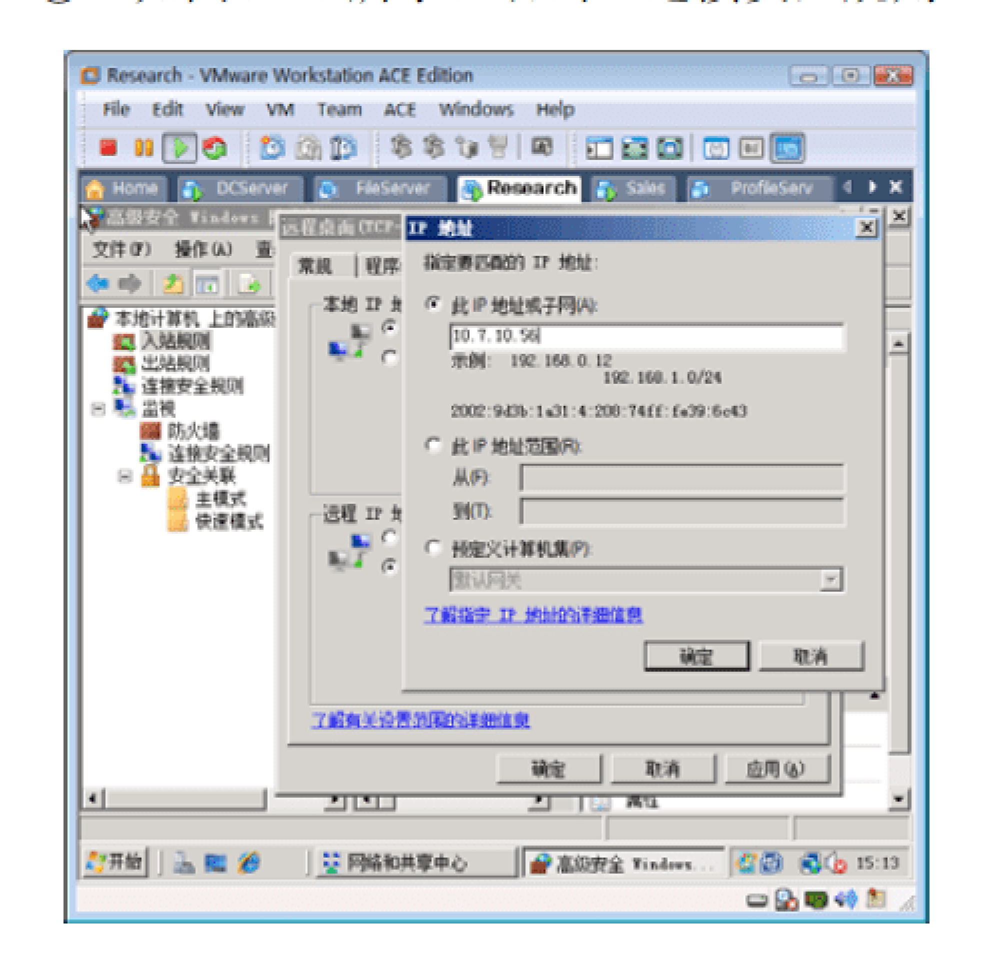


图 9-69　指定 IP 地址

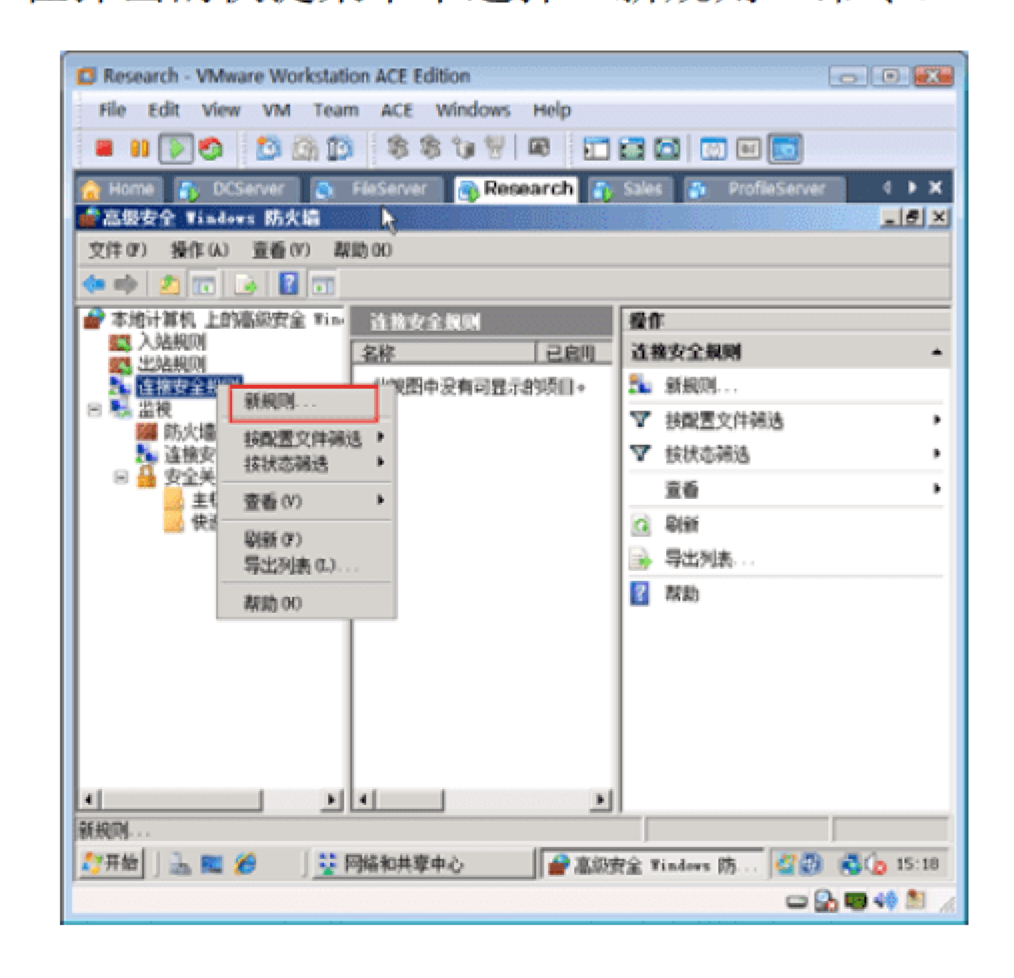


图 9-70　创建连接安全规则

⑨ 如图 9-71 所示，在“规则类型”界面中，选中“服务器到服务器”单选按钮，单击“下一步”按钮。

⑩ 如图 9-72 所示，在“终结点”界面中，终结点 2 中的计算机下选中“下列 IP 地址”单选按钮。单击“添加”按钮，添加 10.7.10.125 和 10.7.10.56。

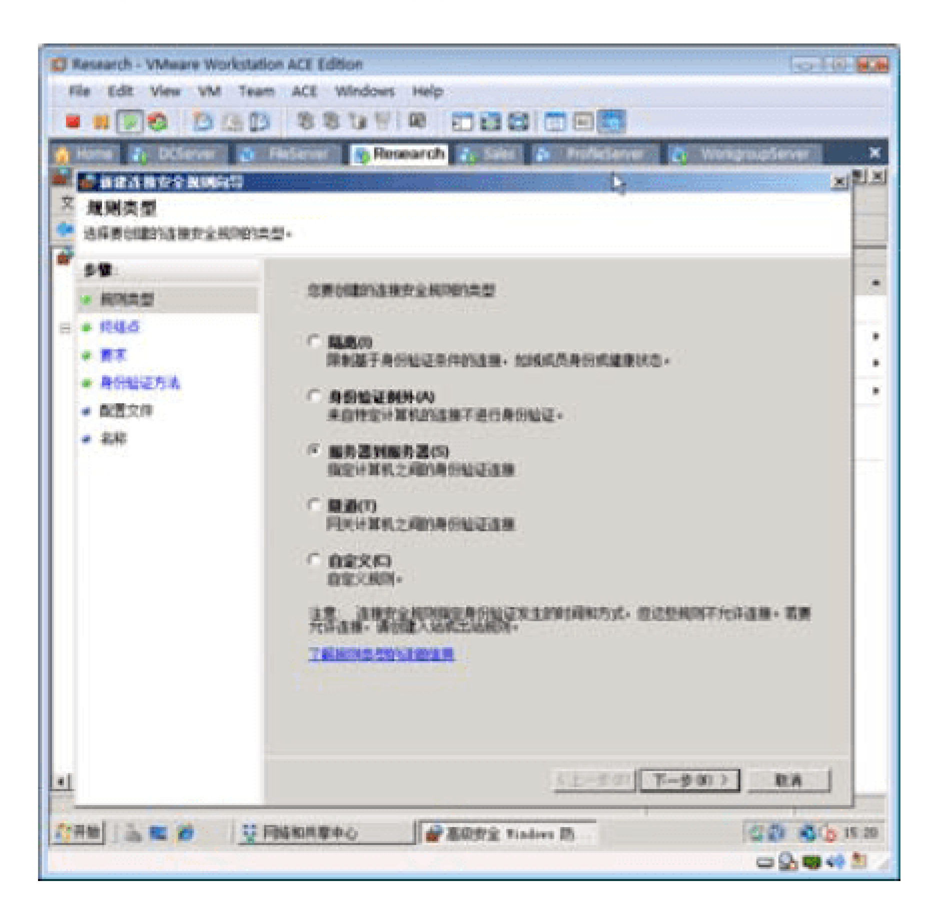


图 9-71　“规则类型”界面

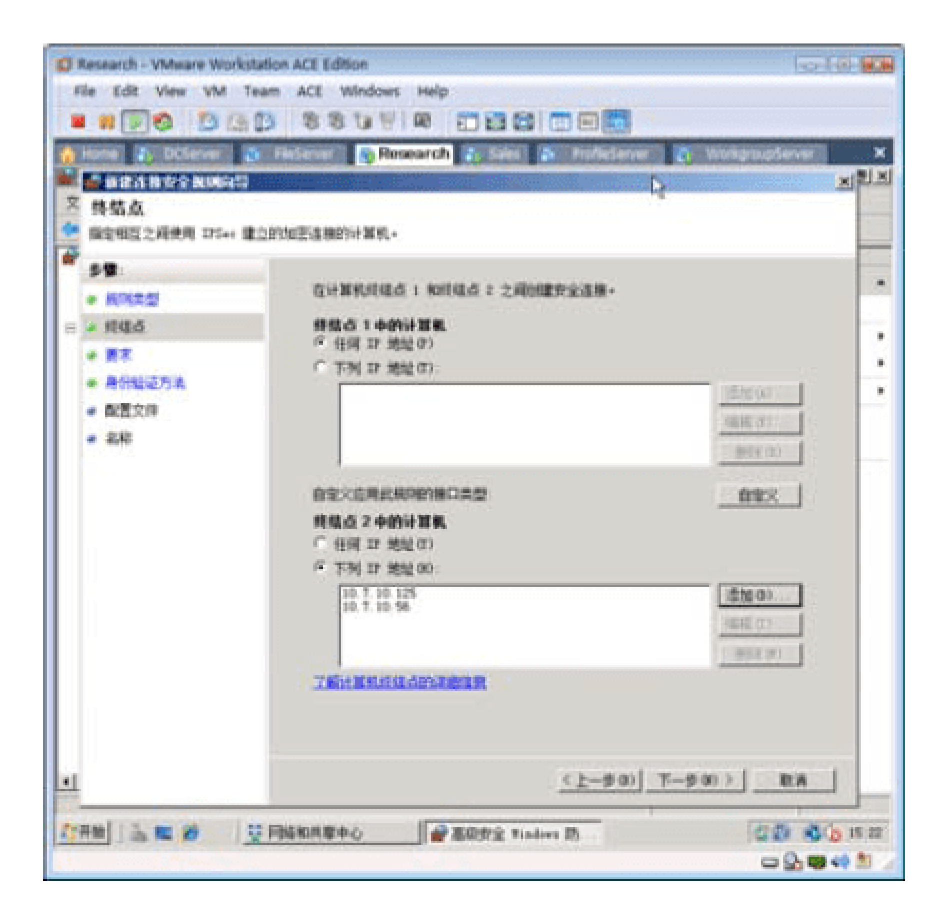


图 9-72　“终结点”界面

⑪ 如图 9-73 所示，在“要求”界面中，选中“入站和出站连接要求身份验证”单选按钮，单击“下一步”按钮。

⑫ 如图 9-74 所示，在“身份验证方法”界面中，选中“自定义”，单击“自定义”按钮。

⑬ 在自定义高级身份验证对话框中，选中“第一身份验证可选”复选框，单击“添加”按钮。

⑭ 选中“计算机(Kerberos v5)”单选按钮，单击“确定”按钮，如图 9-75 所示。

⑮ 如图 9-76 所示，再次单击“添加”按钮，选择“预共享密钥”单选按钮，单击“确定”按钮。

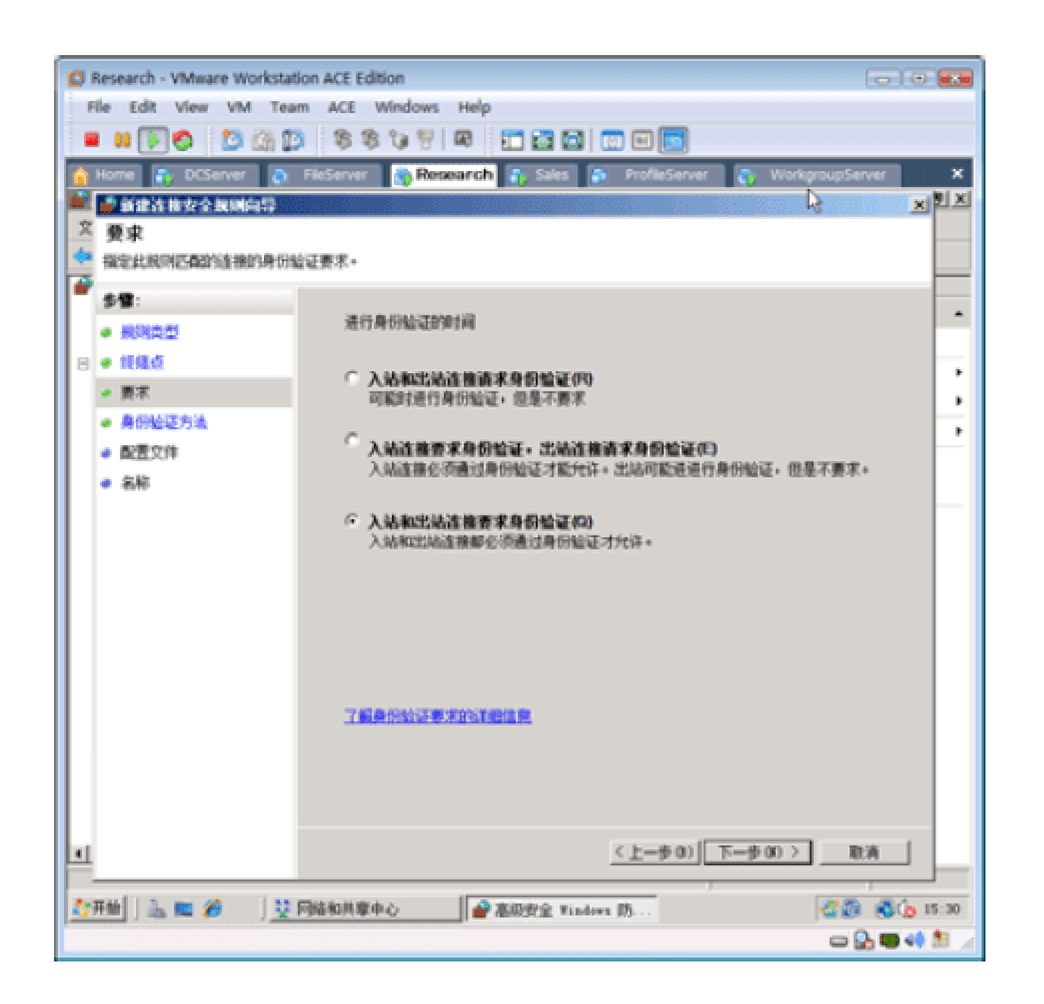


图 9-73　指定要求

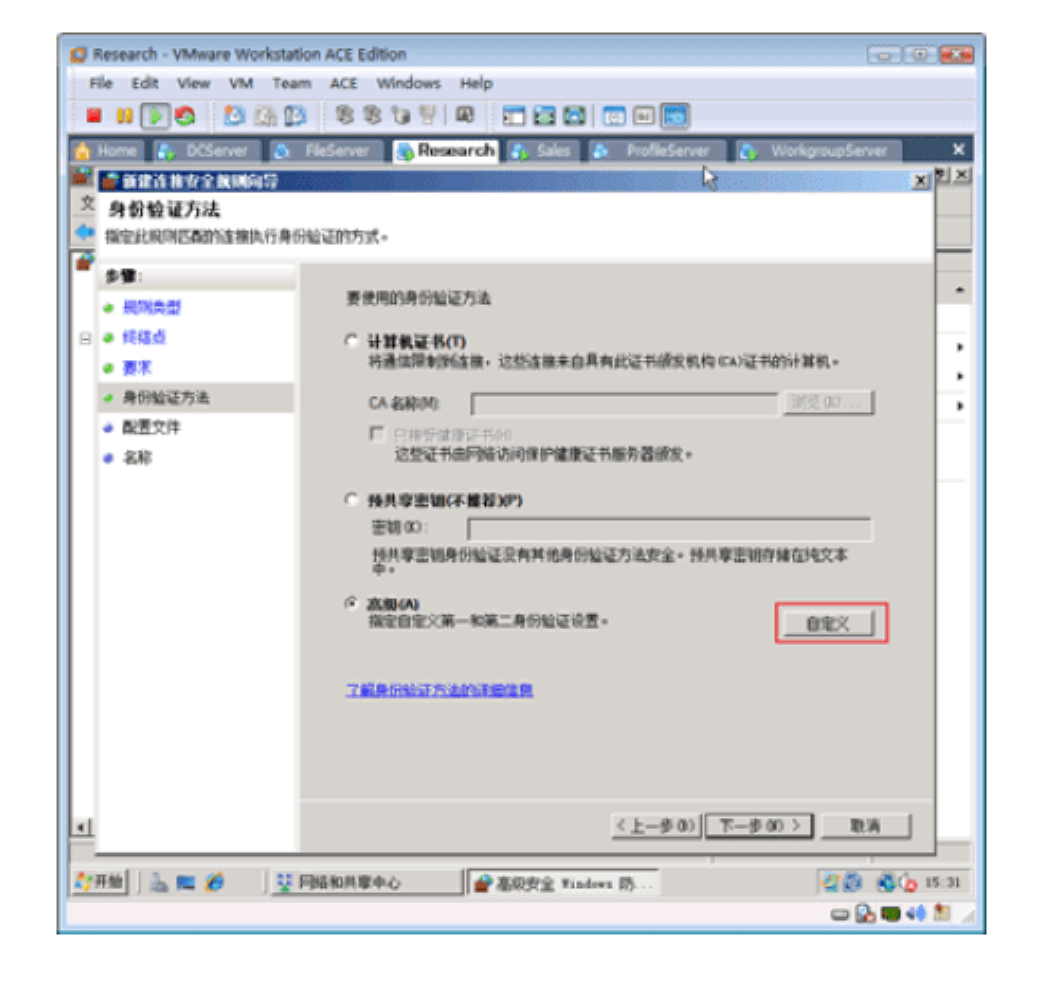


图 9-74　“身份验证方法”对话框



提示：Kerberos 身份验证是针对域中计算机 Sales 设置的，预共享密钥身份验证是针对 WorkgroupServer 设置的。工作组之间身份验证要么使用计算机证书，要么使用预共享密钥。

警告：建议不要将第一身份验证和第二身份验证都配置为可选，否则，这样的配置等同于关闭身份验证。

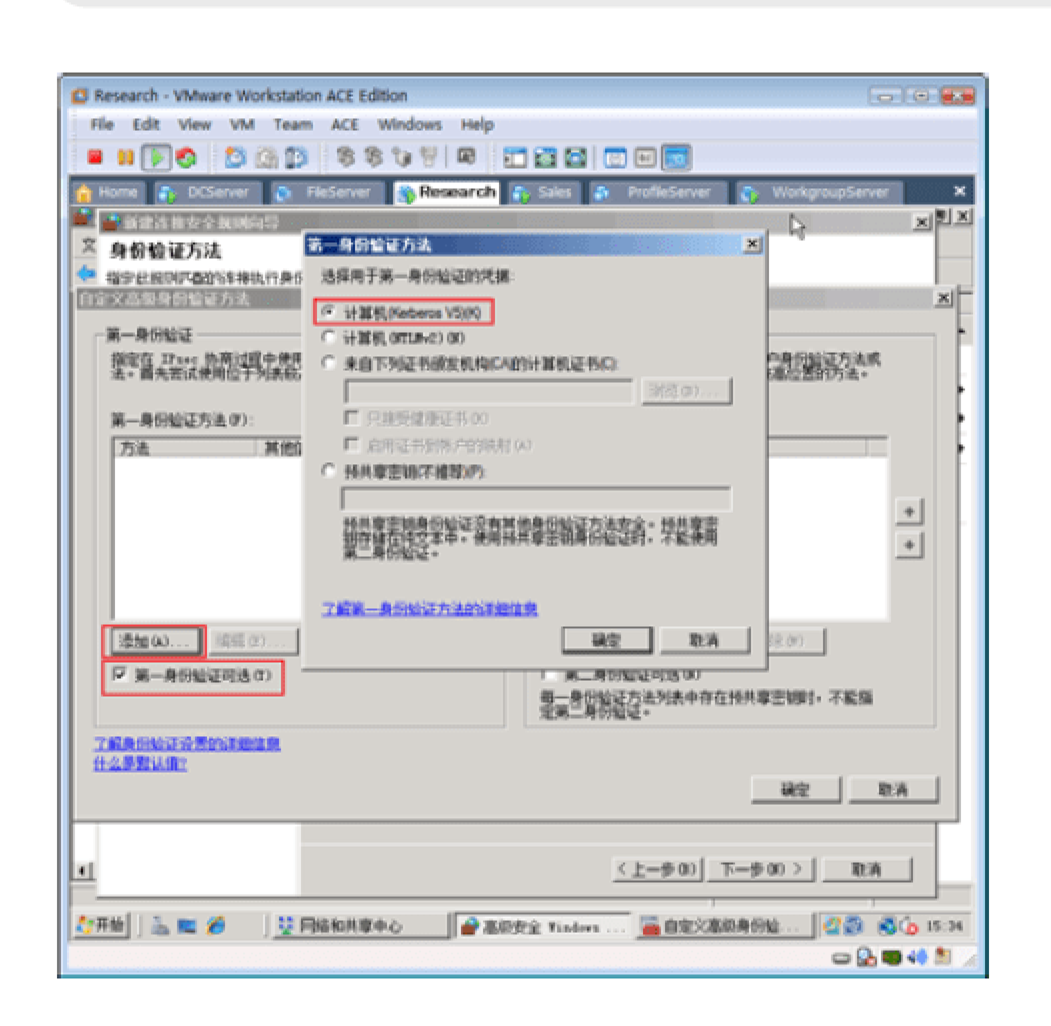


图 9-75　指定身份验证方法(一)

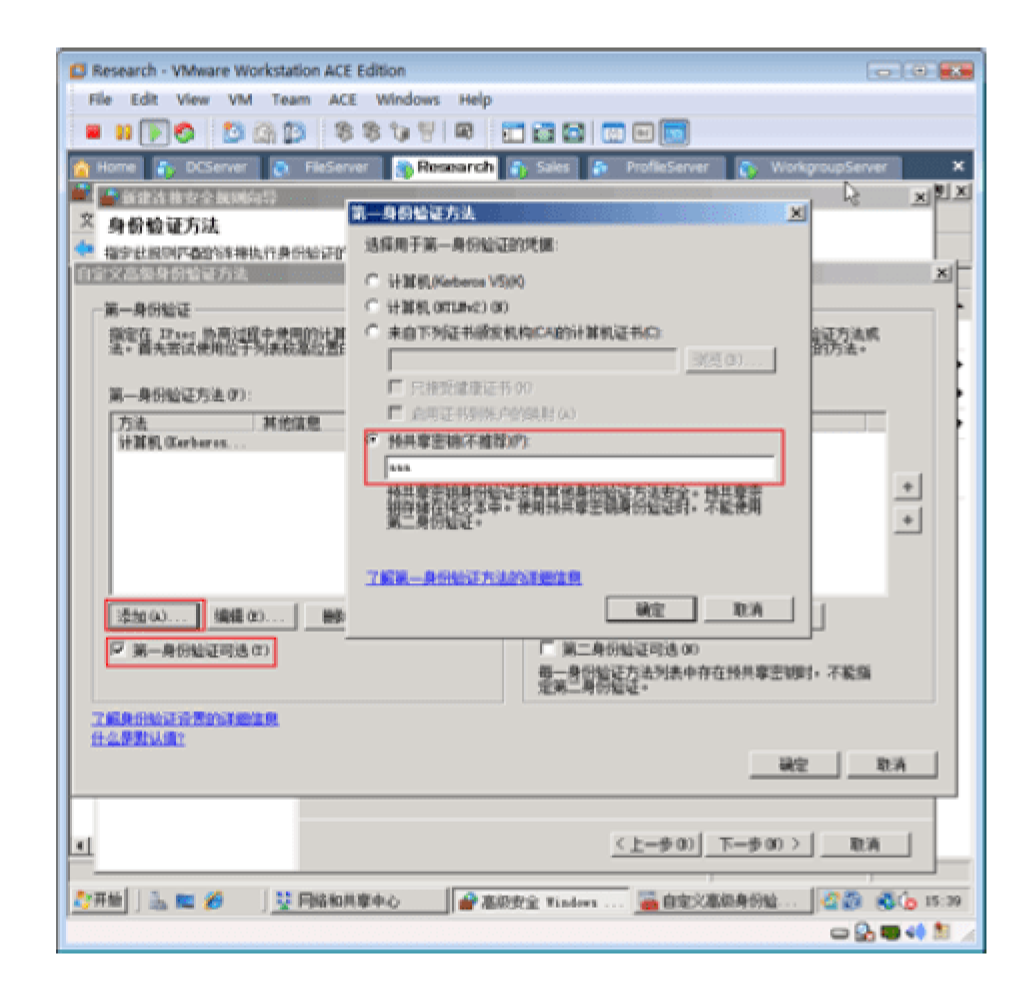


图 9-76　指定身份验证方法(二)

⑯ 如图 9-77 所示，在“配置文件”界面中，只选中“域”复选框，单击“下一步”按钮。

⑰ 如图 9-78 所示，在“名称”界面中，输入“RDP 连接安全规则”，单击“完成”按钮。

⑱ 以管理员身份登录 Sales，选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 wf.msc，打开高级 Windows 防火墙。

⑲ 如图 9-79 所示，单击“出站规则”，单击“新规则”按钮。

⑳ 如图 9-80 所示，在“规则类型”界面中，选中“自定义”单选按钮，单击“下一步”按钮。

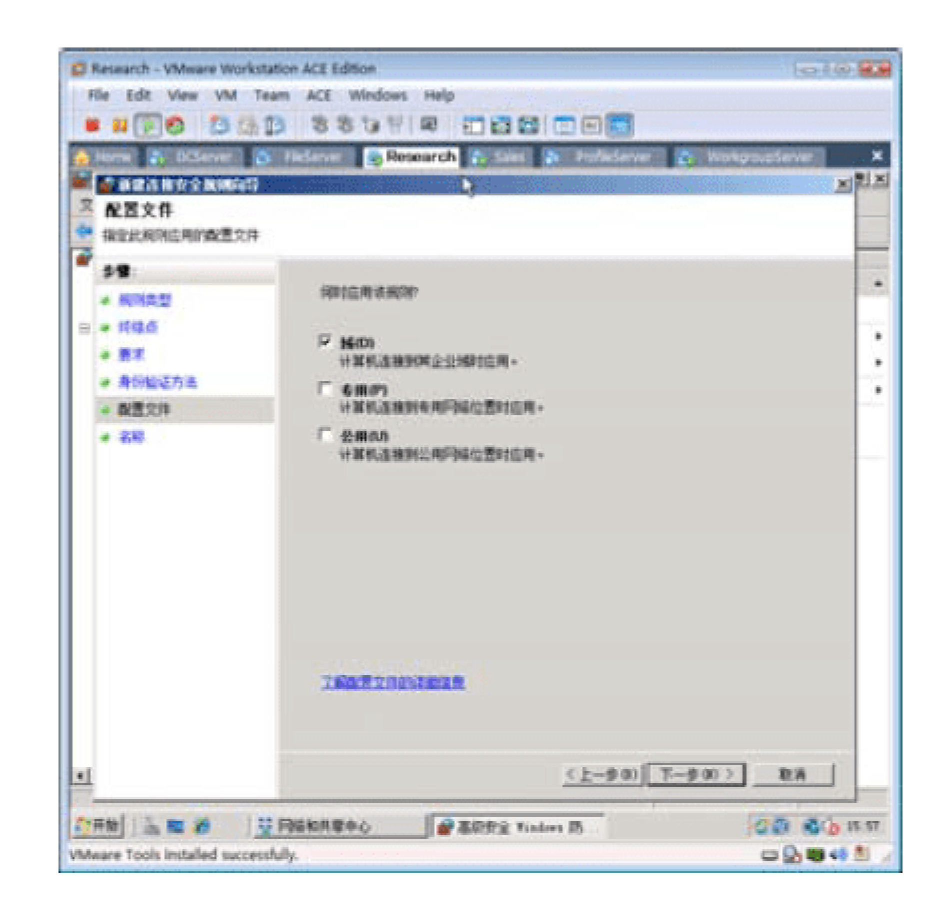


图 9-77　指定配置文件

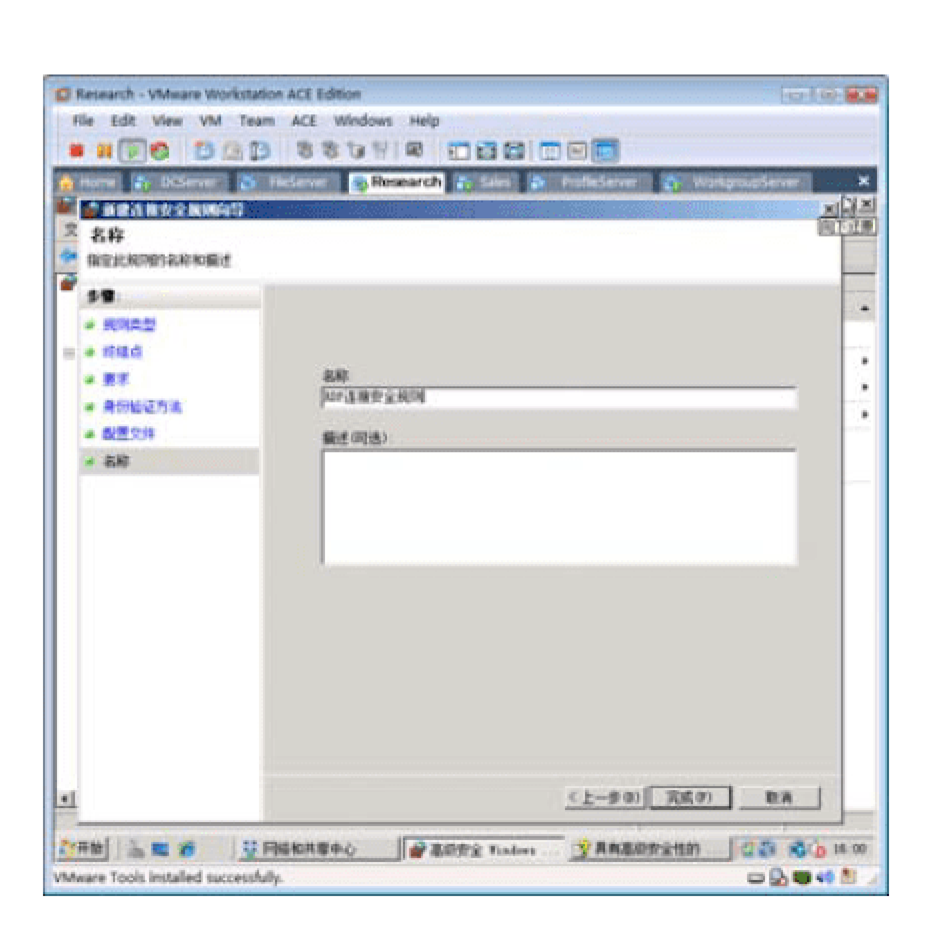


图 9-78　指定名称

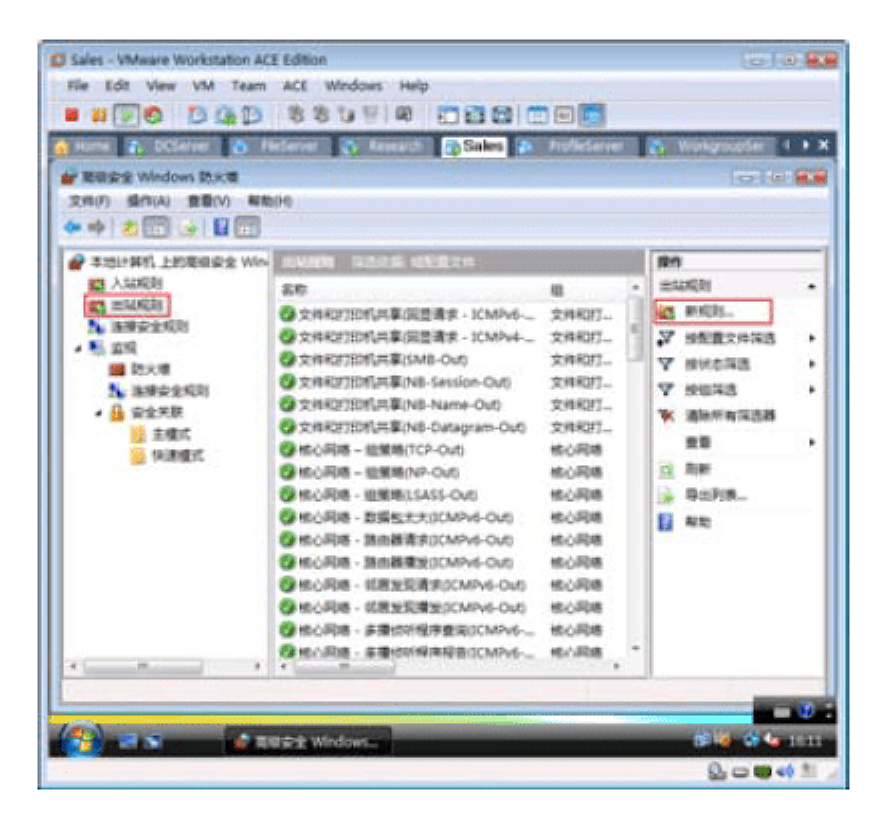


图 9-79　新建出站规则

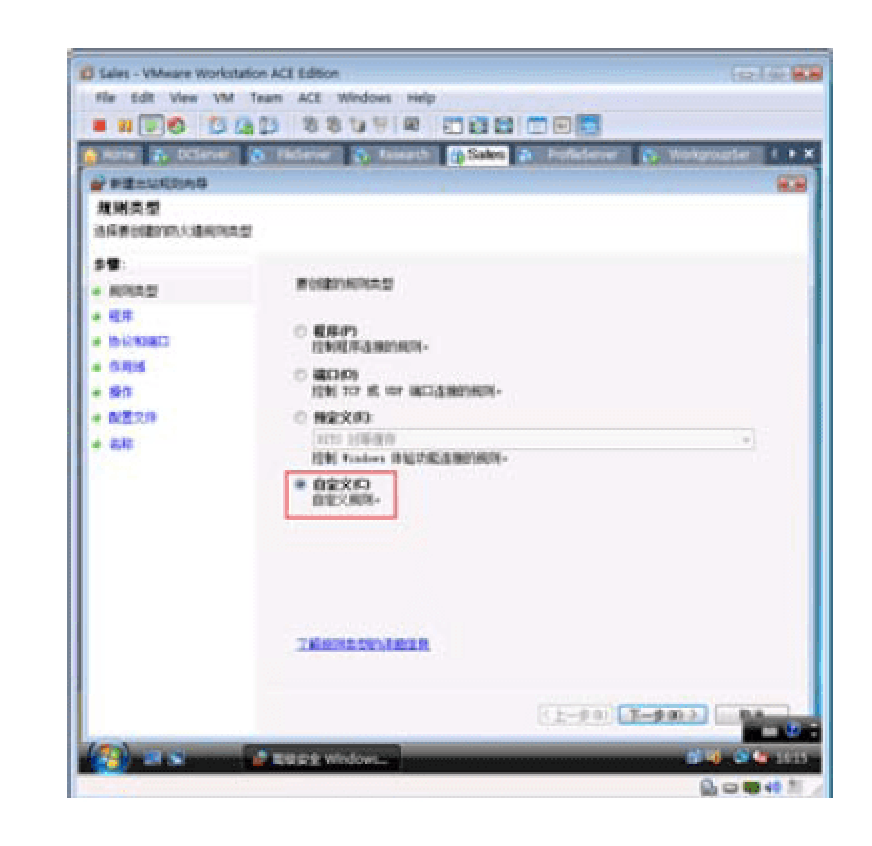


图 9-80　定义规则类型

㉑ 如图 9-81 所示，在“程序”界面中，选中“所有程序”单选按钮，单击“下一步”按钮。

㉒ 如图 9-82 所示，在“协议和端口”界面中，协议类型选择 TCP，远程端口输入 3389，单击“下一步”按钮。

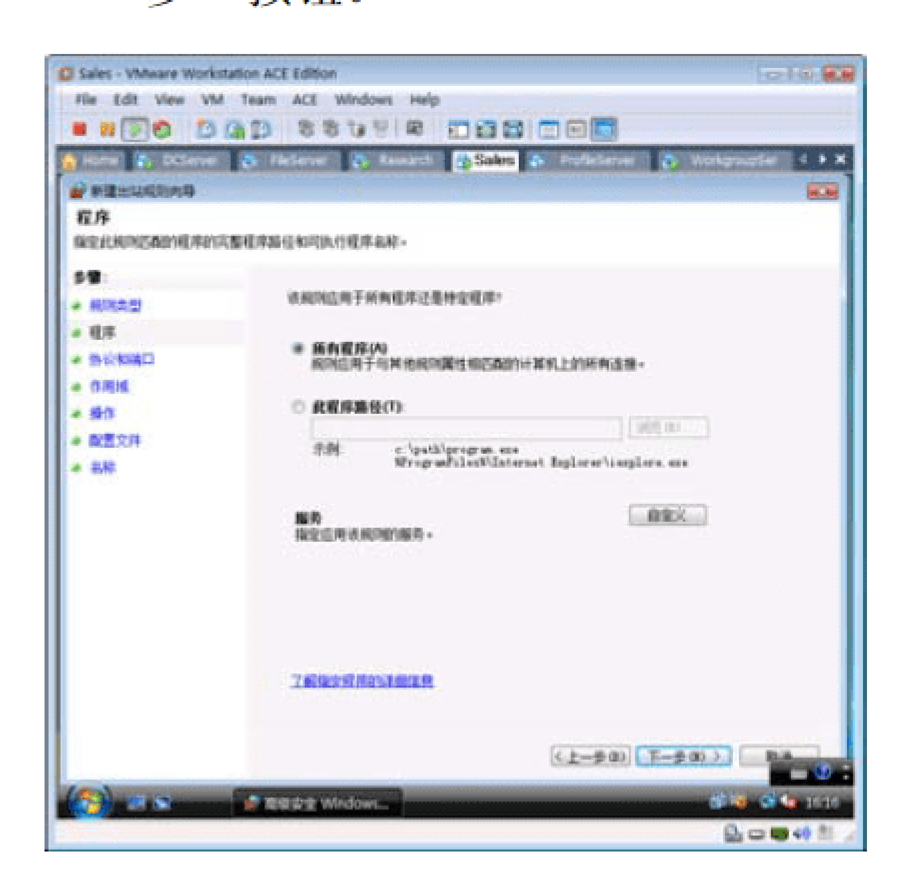


图 9-81　指定程序

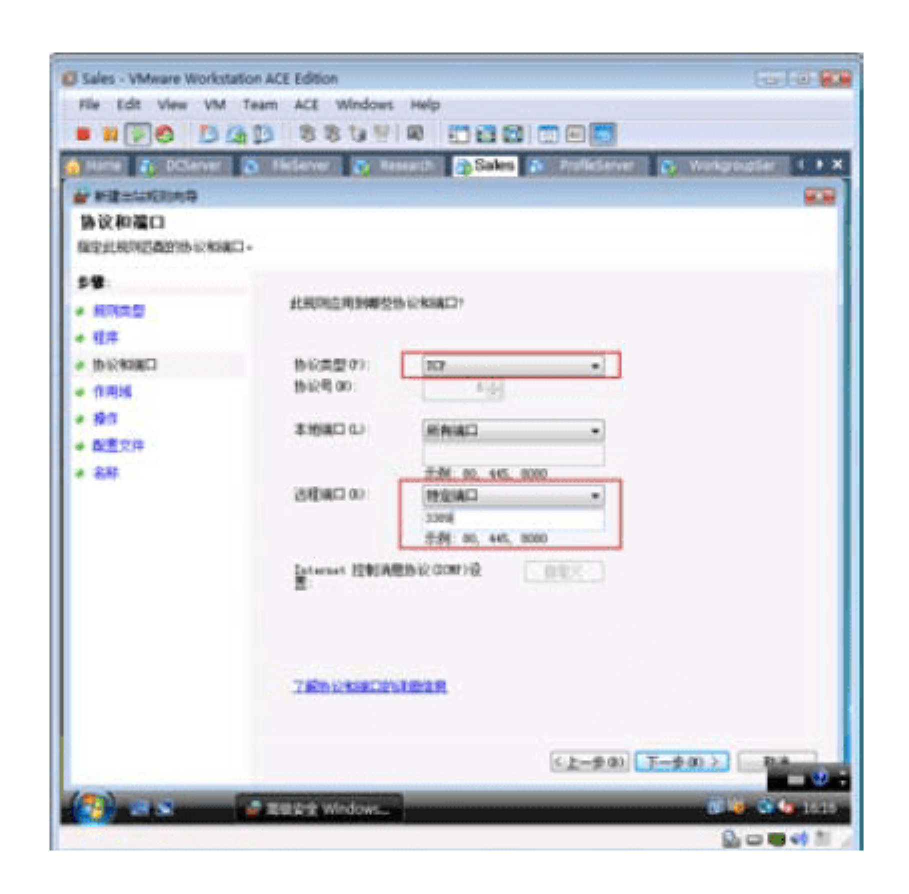


图 9-82　指定协议和端口

㉓ 如图 9-83 所示，在“作用域”界面中，添加 10.7.10.40，单击“下一步”按钮。

㉔ 如图 9-84 所示，在“操作”界面中，选中“只允许安全连接”单选按钮，选中“要求加密连接”复选框，单击“下一步”按钮。

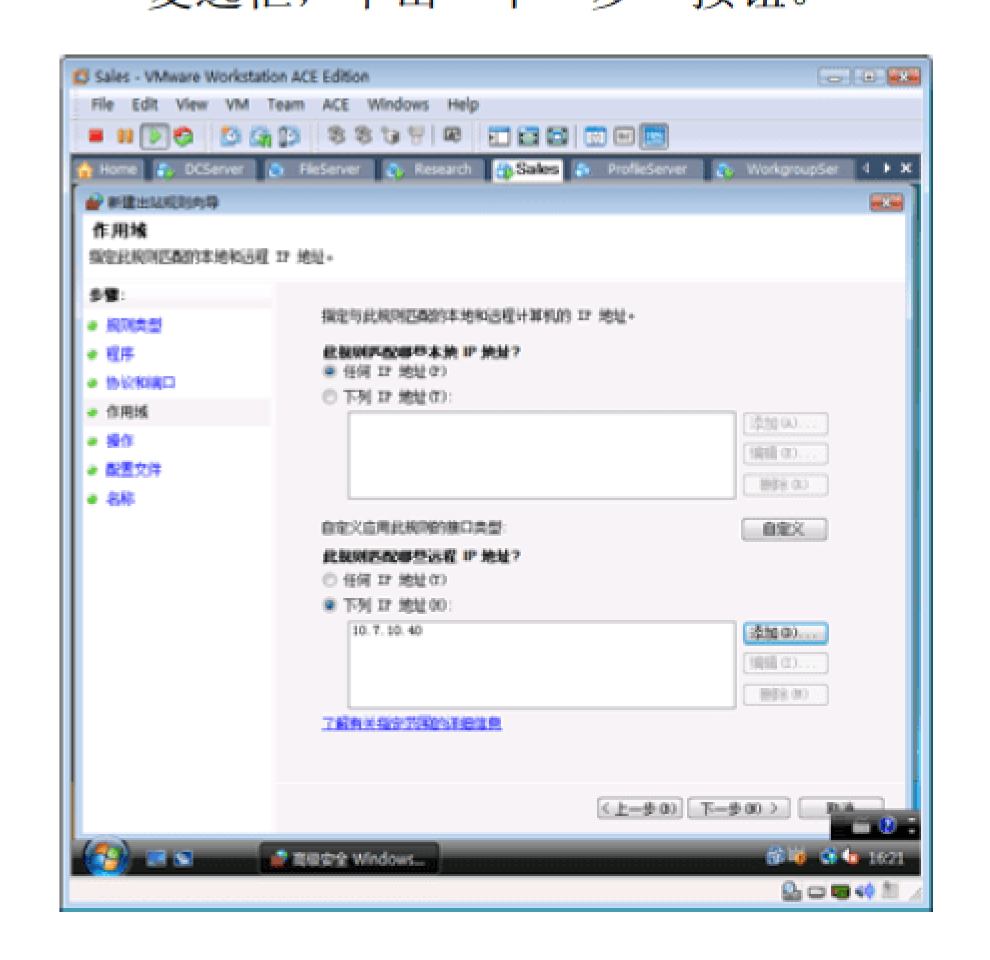


图 9-83 指定作用域

图 9-84 指定操作

㉕ 如图 9-85 所示，在出现的“计算机”界面中，单击“下一步”按钮。

㉖ 如图 9-86 所示，在出现的“名称”界面中，输入规则名，单击“完成”按钮。

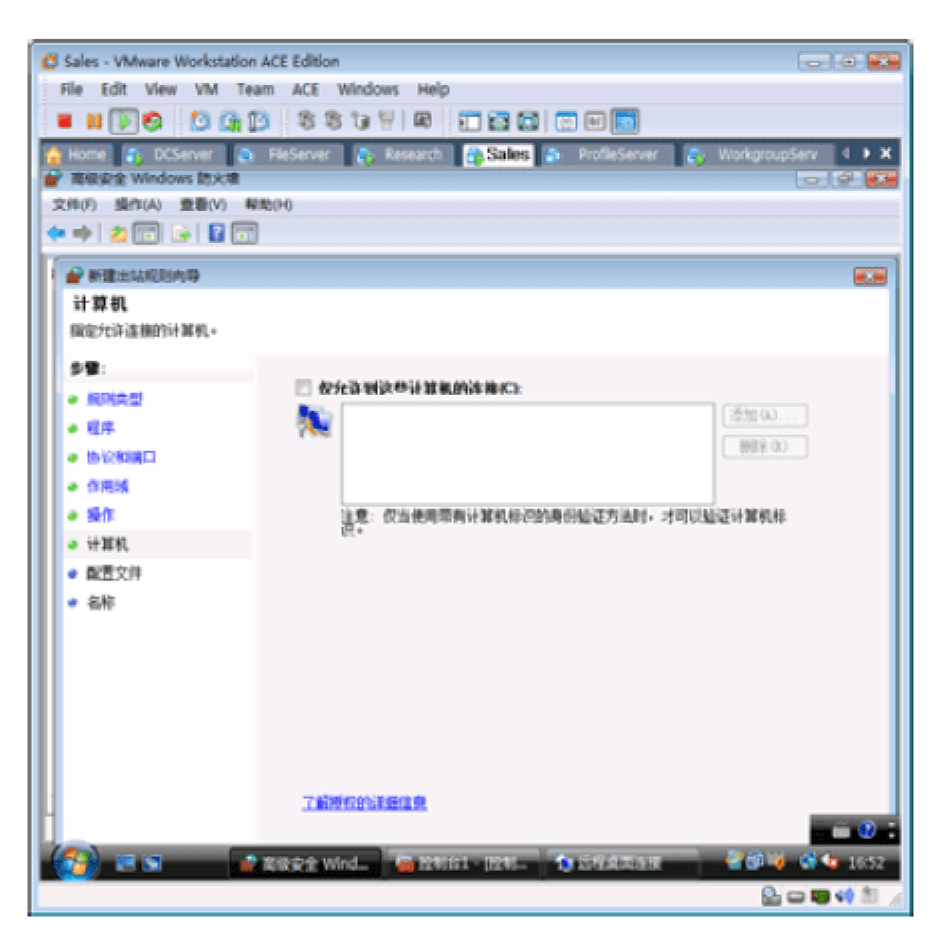


图 9-85 指定计算机

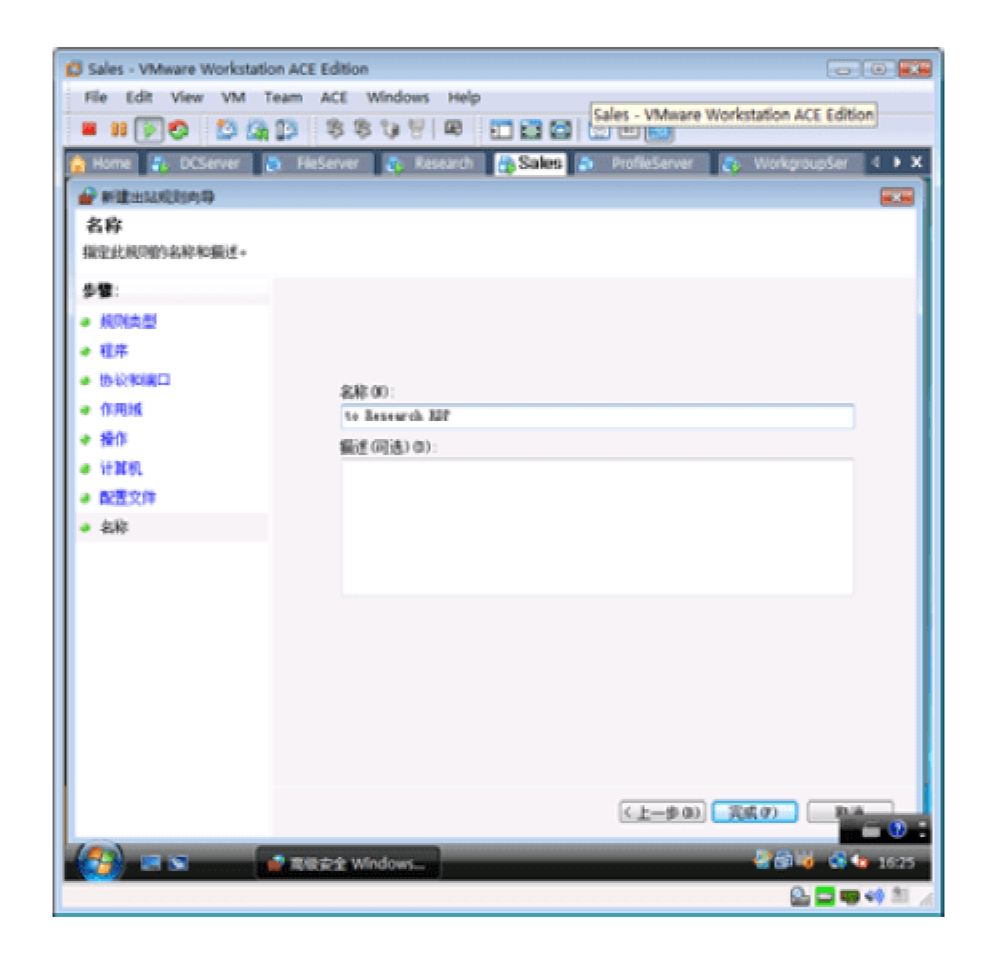


图 9-86 指定规则名称

㉗ 如图 9-87 所示，创建连接安全规则。在“规则类型”界面中，选中“服务器到服务器”单选按钮，单击“下一步”按钮。

㉘ 如图 9-88 所示，在“终结点”界面中，输入 10.7.10.40，单击“下一步”按钮。

㉙ 如图 9-89 所示，在“要求”界面中，选中“入站和出站连接要求身份验证”单选按钮，单击“下一步”按钮。

㉚ 如图 9-90 所示，在“身份验证方法”界面中，选中“高级”单选按钮，单击“自定义”按钮。

㉛ 如图 9-91 所示，在自定义高级身份验证对话框中，选中“第一身份验证可选”复选框，单击“添加”按钮。选中“计算机(Kerberos v5)”单选按钮，单击“确定”按钮。

㉜ 如图 9-92 所示，在“配置文件”界面中，只选中“域”复选框，单击“下一步”按钮。

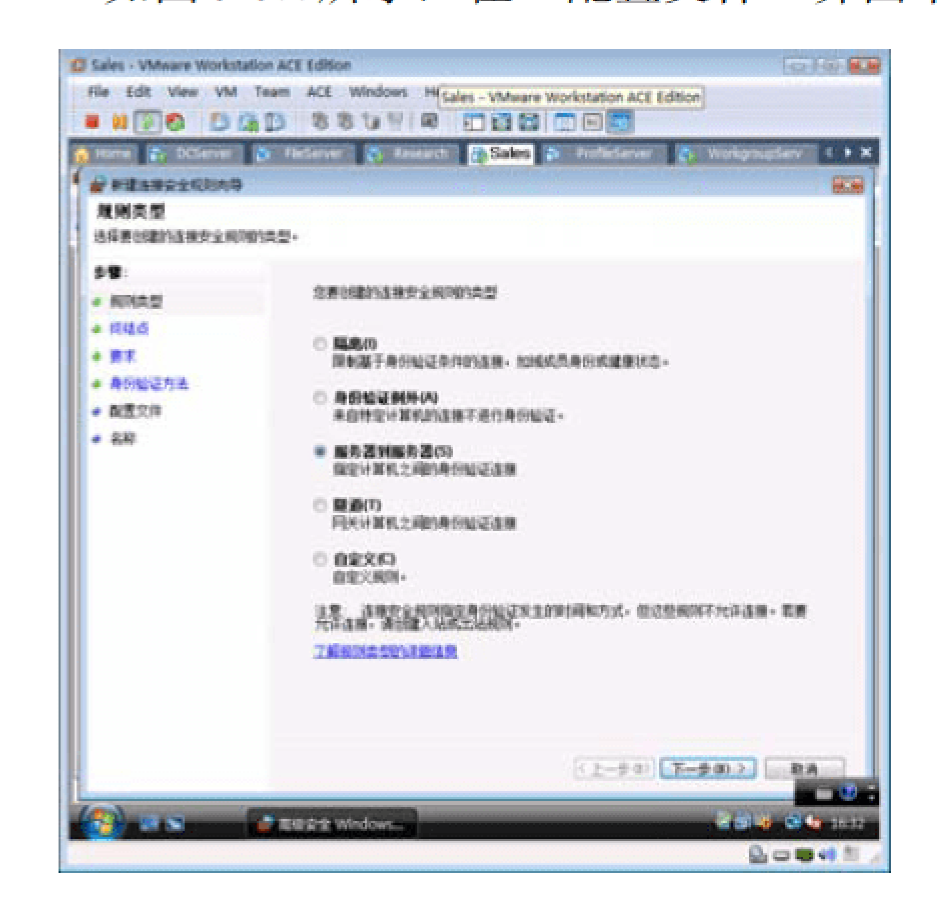


图 9-87 指定规则类型



图 9-88 指定终结点

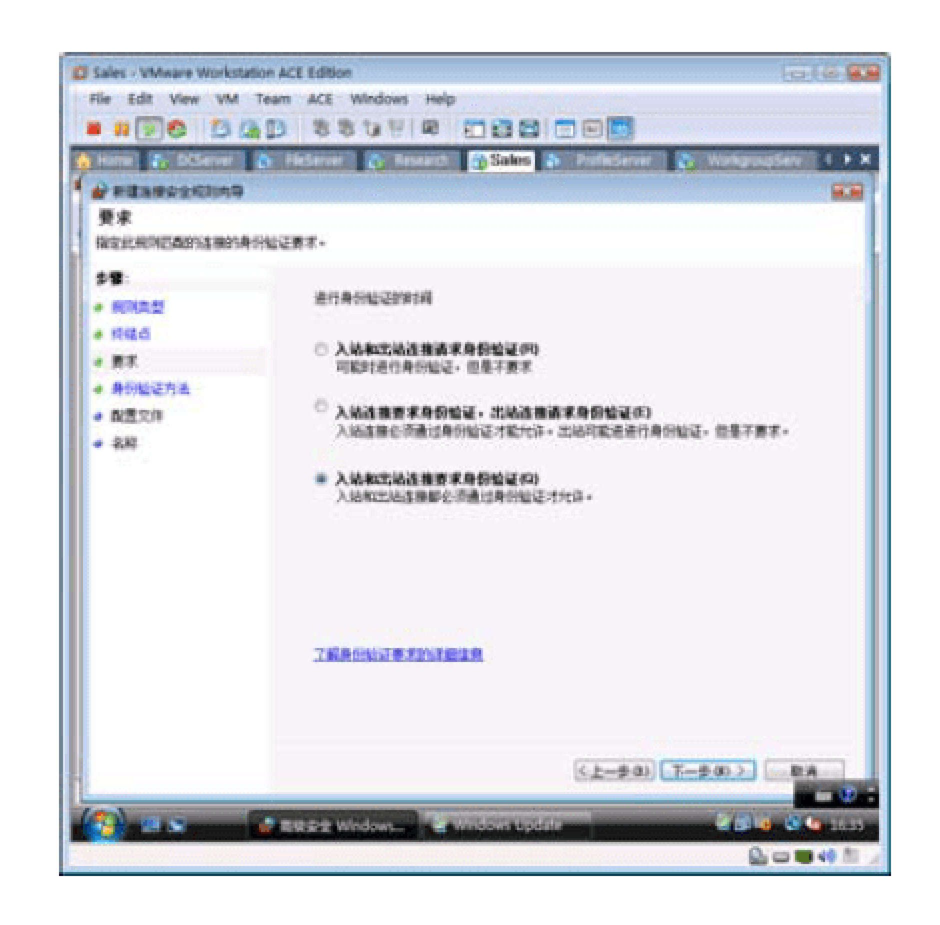


图 9-89 指定要求

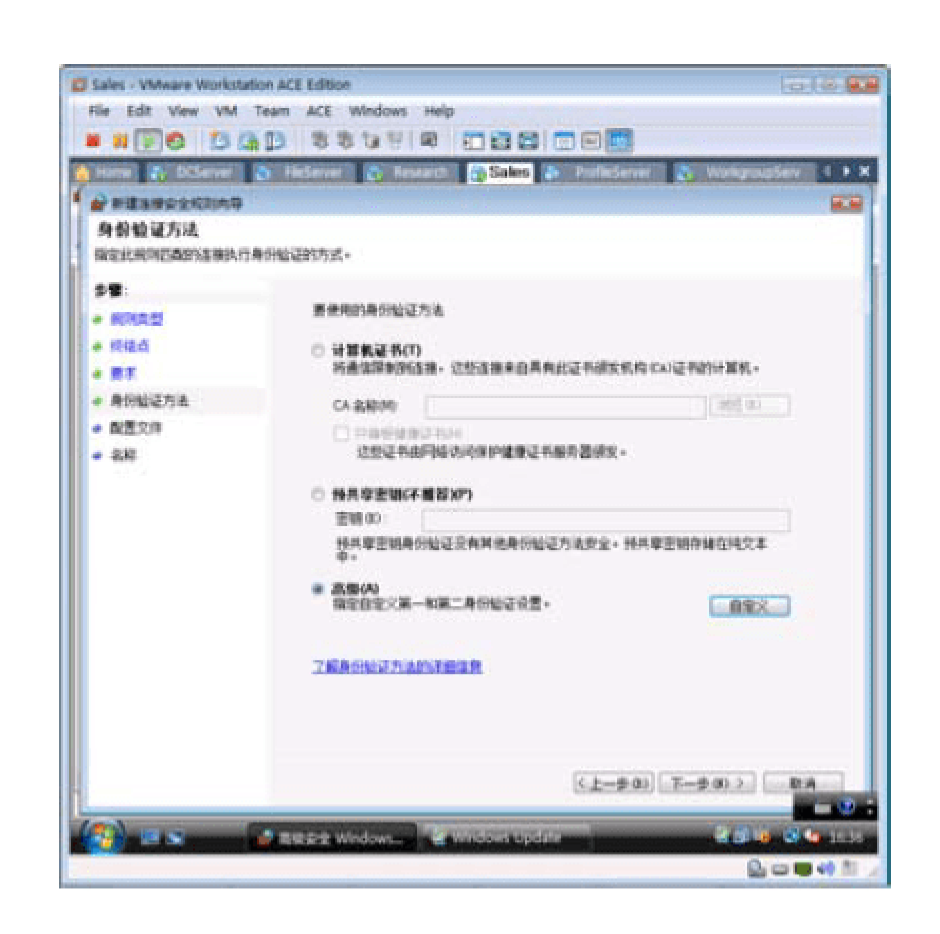


图 9-90 指定身份验证方法(一)

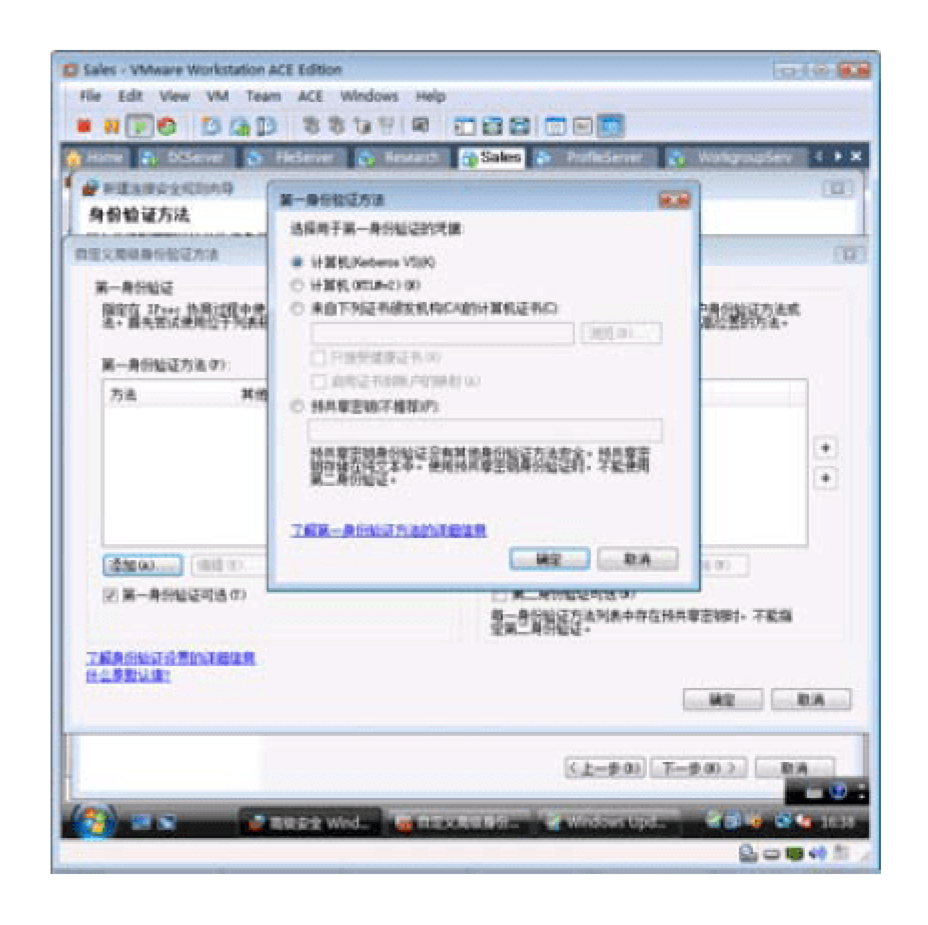


图 9-91 指定身份验证方法(二)

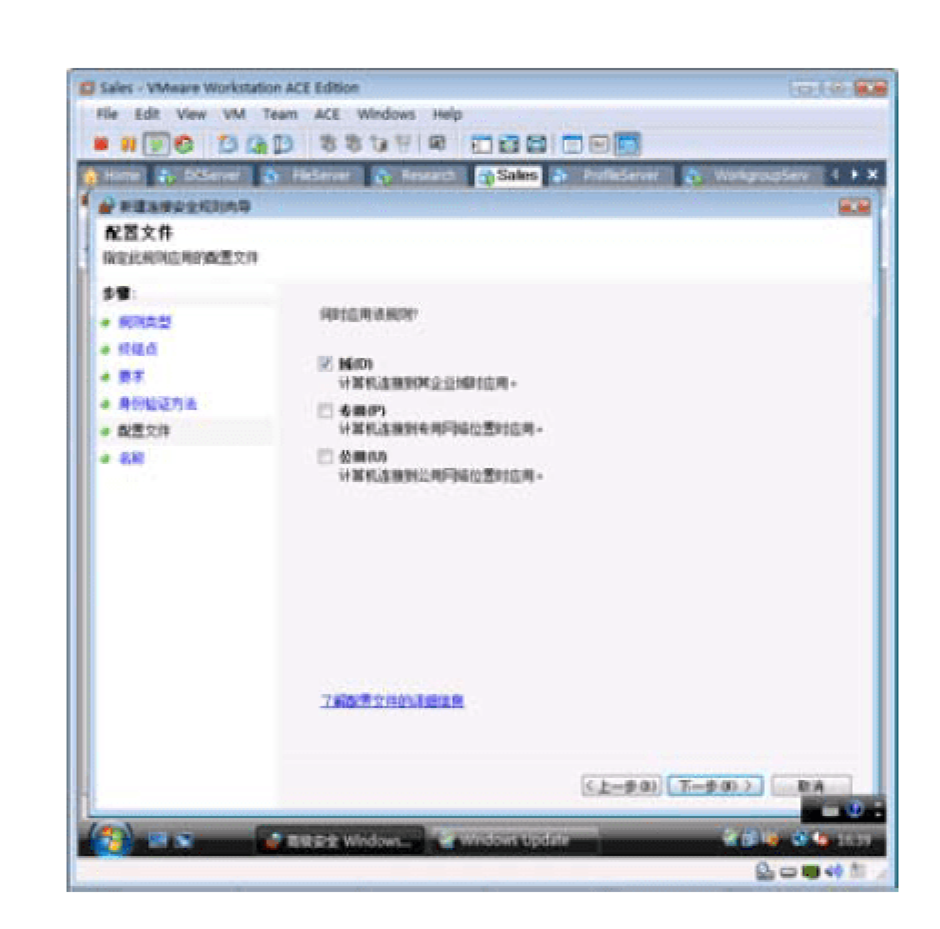


图 9-92 指定配置文件

㉝ 如图 9-93 所示，在“名称”界面中，输入名称，单击“完成”按钮。

㉞ 如图 9-94 所示，选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 mstsc，打开远程桌面客户端，输入 Research，单击“连接”按钮。使用 Kerberos 身份验证能够成功。

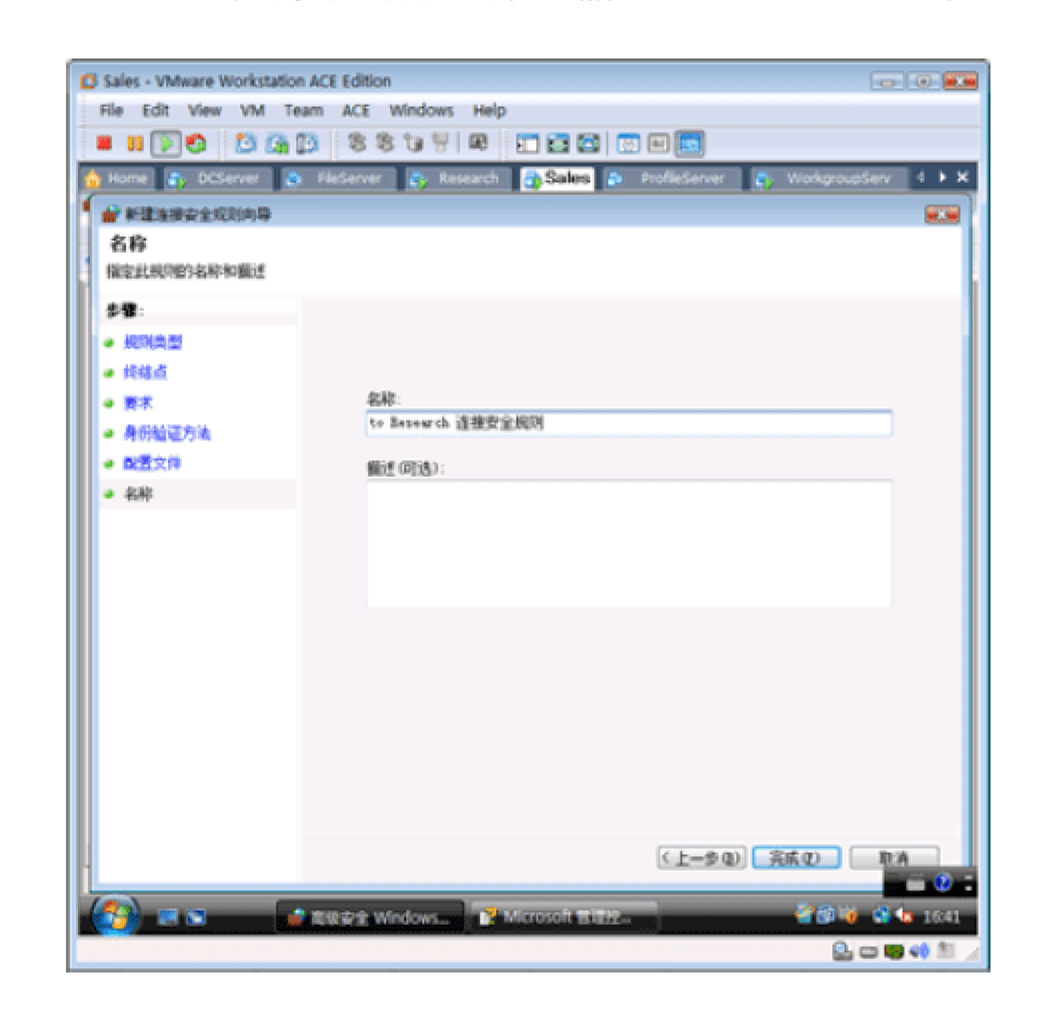


图 9-93　输入名称

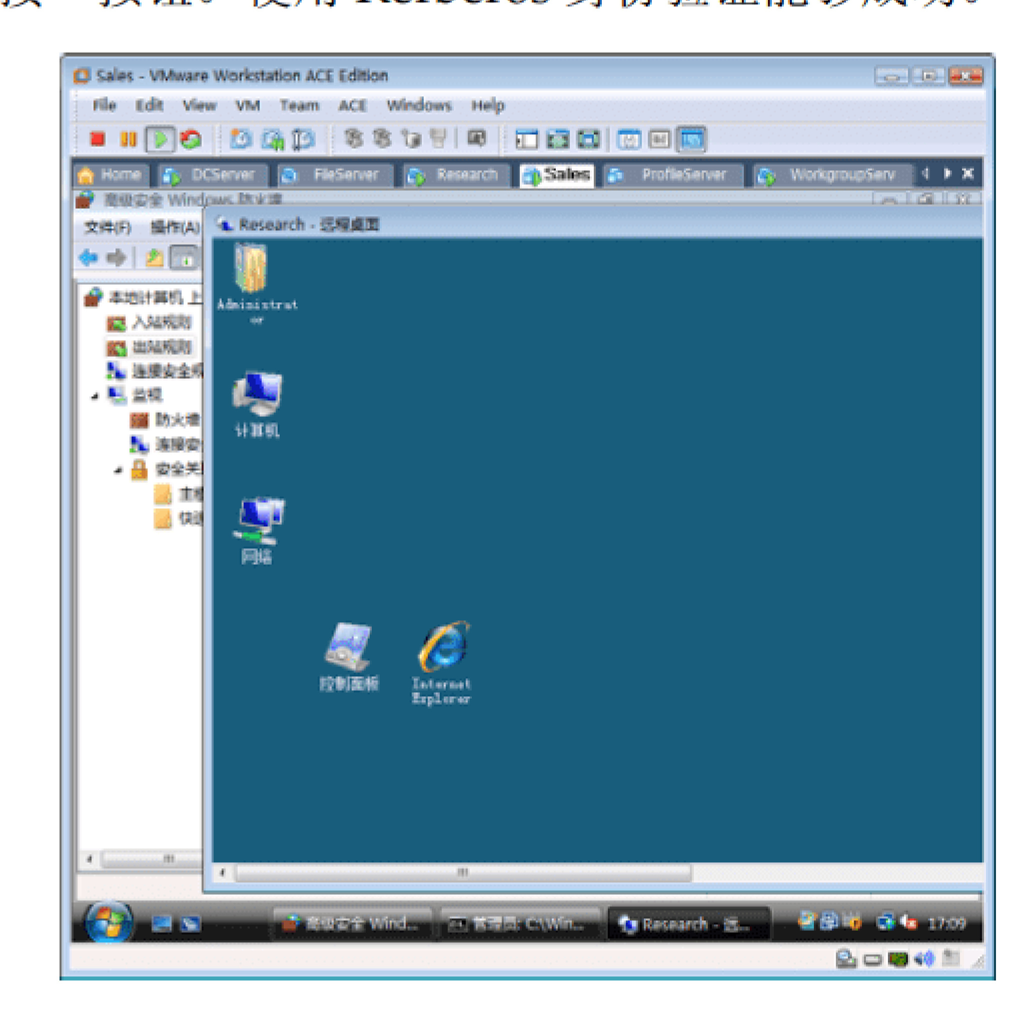


图 9-94　测试规则

㉟ 在 WorkgroupServer 上，参照在 Sales 上的配置。配置高级 Windows 防火墙，创建到 Research 计算机的出站规则，再创建连接安全规则，身份验证选择“预共享密钥”，如图 9-95 所示。

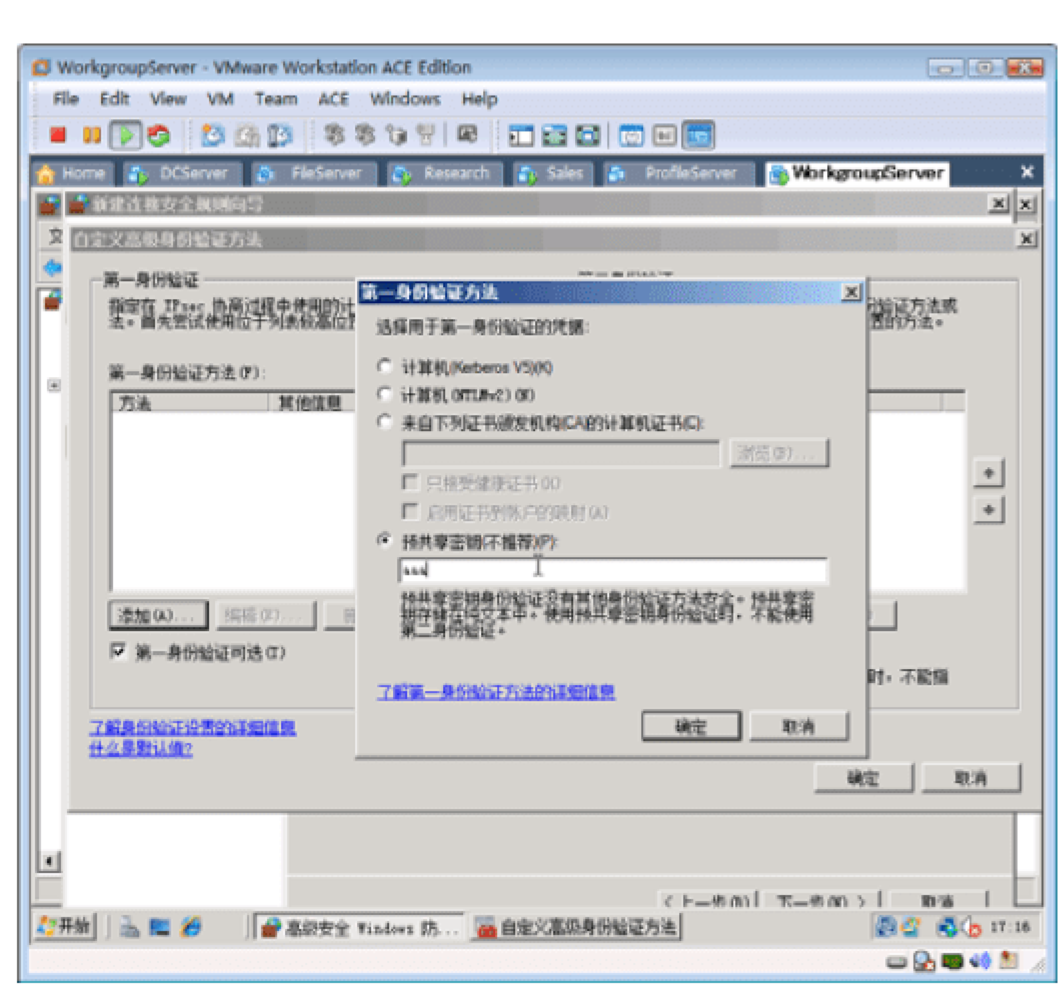


图 9-95　设置身份验证方法

9.6.6　示例：监视加密通信

监视节点显示有关当前所连接的计算机(本地计算机或远程计算机)的信息。如果使用管理单元来管理组策略对象而不是本地计算机，则不会出现该节点。

确保 Sales 计算机和 WorkgroupServer 计算机使用远程桌面连接到 Research 计算机，在 Research 计算机上，打开高级安全防火墙，依次展开“监视”→“安全关联”→“主模式”节点，可以看到两个加密

的连接，如图 9-96 所示。

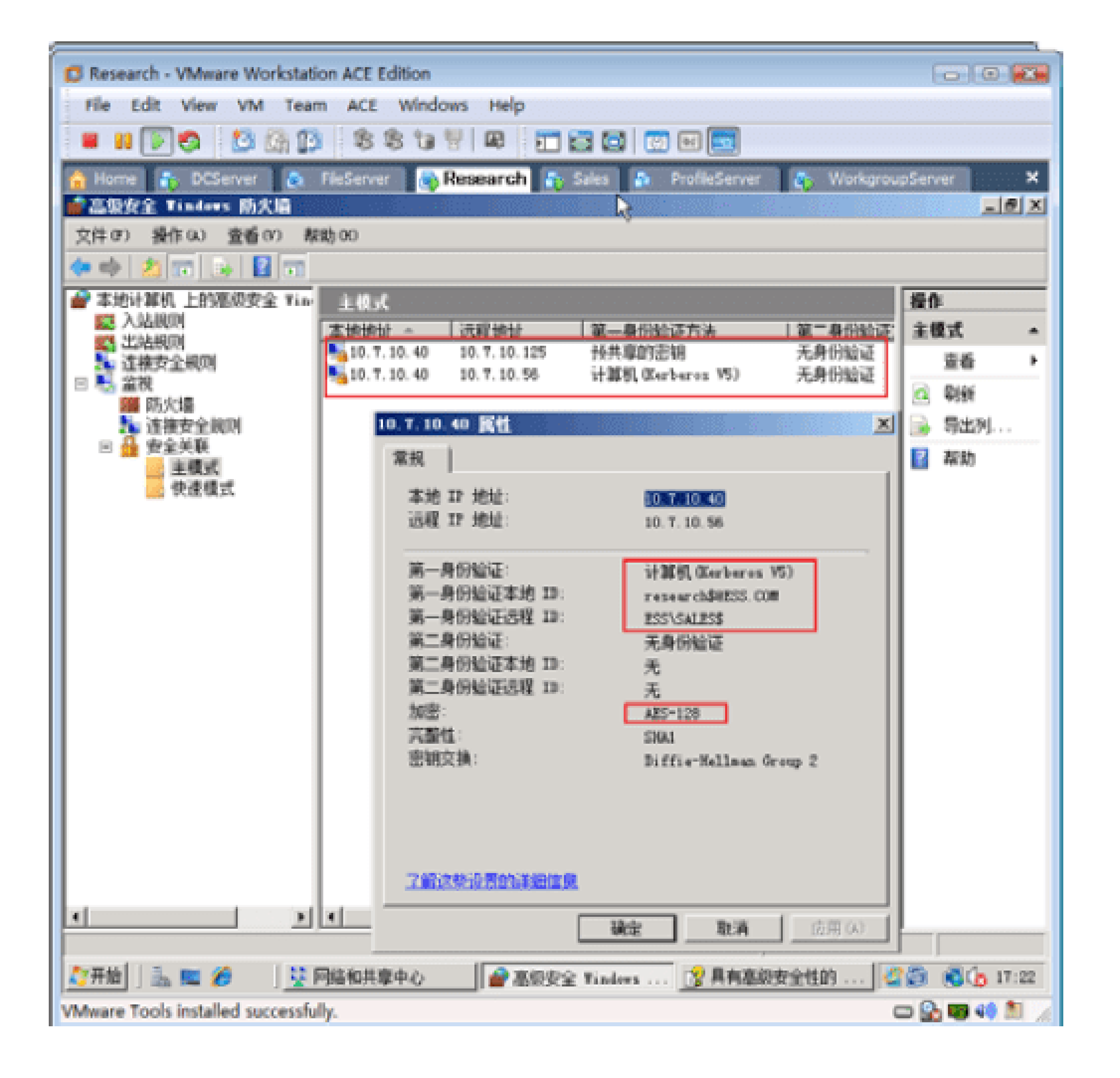


图 9-96　监视 IPSec

9.6.7　配置 IPSec 加密和身份验证的方法

通常情况下使用默认的数据加密和完整性算法最好，你也可以指定自定义的加密和完整性算法。如果使用自定义的数据完整性和加密算法，一定要确保通信两端的完整性和加密算法一致。

① 如图 9-97 所示，右击“本地计算机上的高级安全 Windows 防火墙”，在弹出的快捷菜单中选择“属性”命令。

② 如图 9-98 所示，在“IPSec 设置”选项卡中，单击“自定义”按钮。

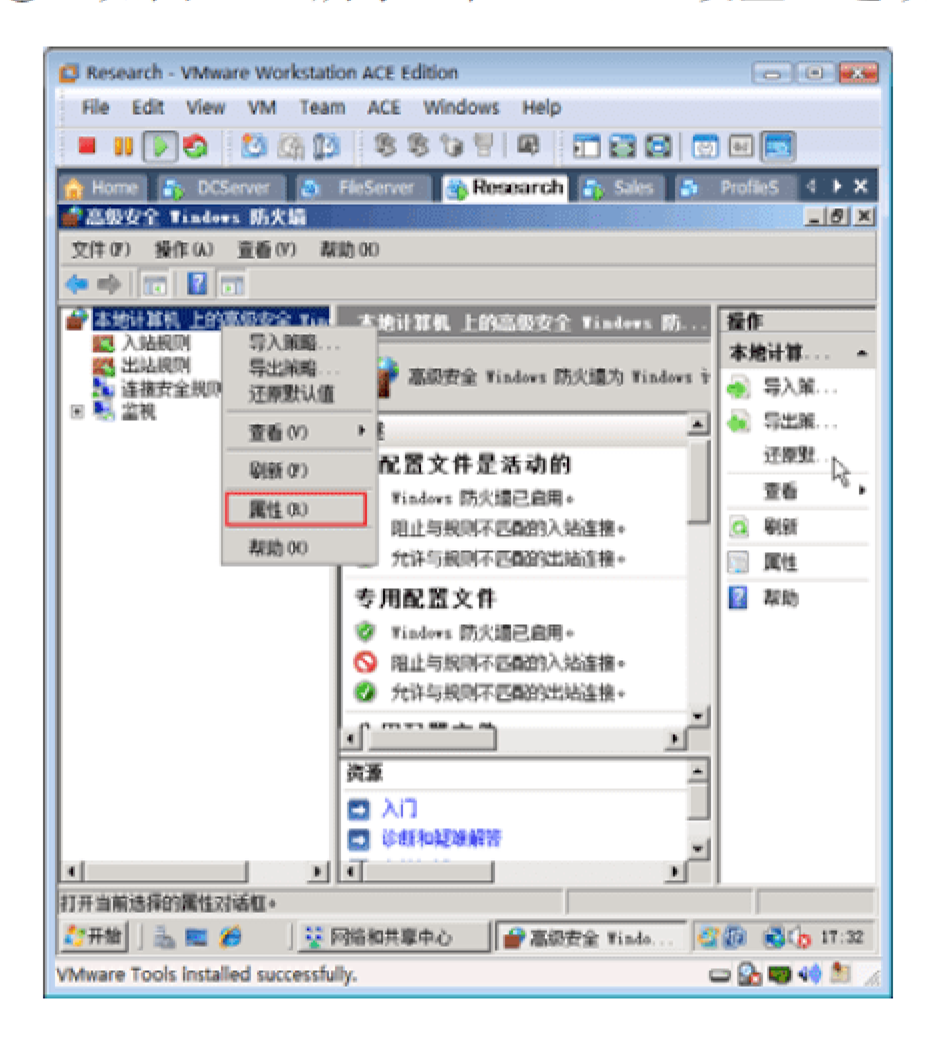


图 9-97　设置 IPSec 身份验证方法(一)

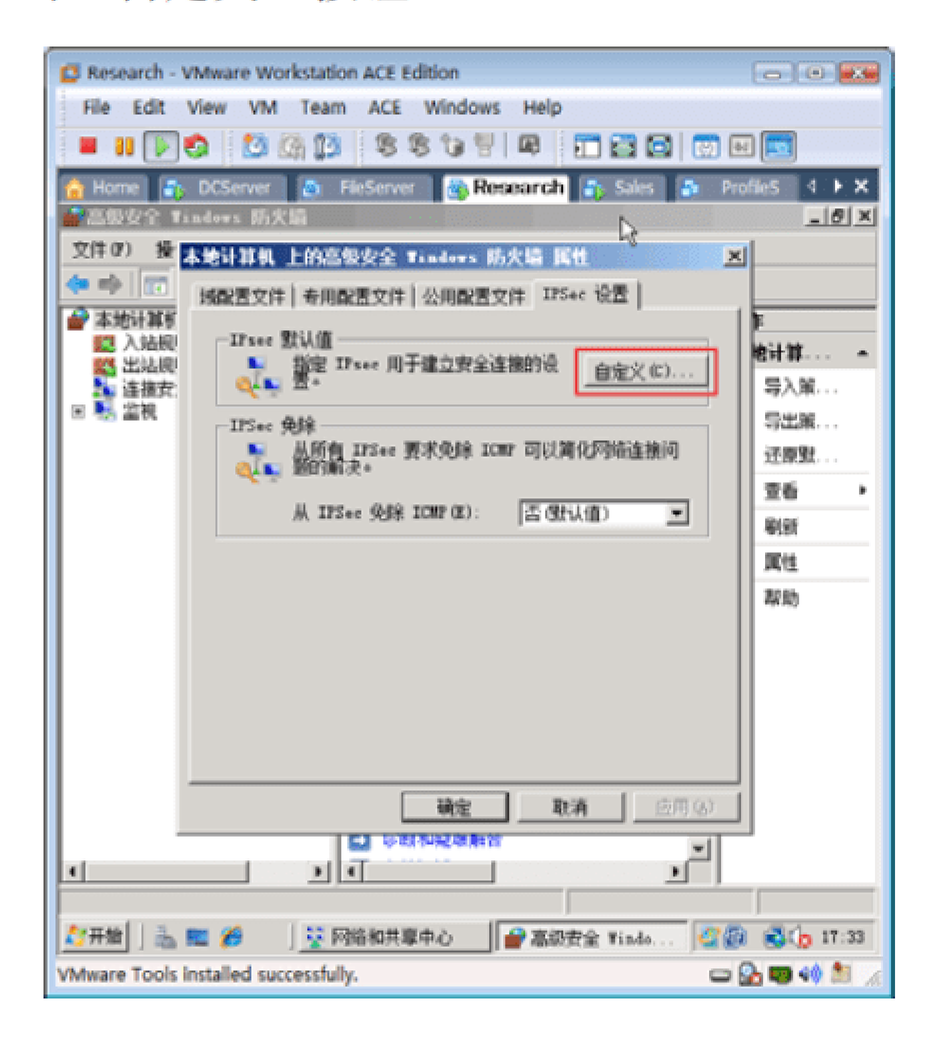


图 9-98　设置 IPSec 身份验证方法(二)

③ 如图 9-99 所示，在“密钥交换”选项区域中，选中“高级”单选按钮，单击“自定义”按钮。

④　如图 9-100 所示，在出现的“自定义高级密钥交换设置”对话框中，可以指定加密算法以及密钥生存期。

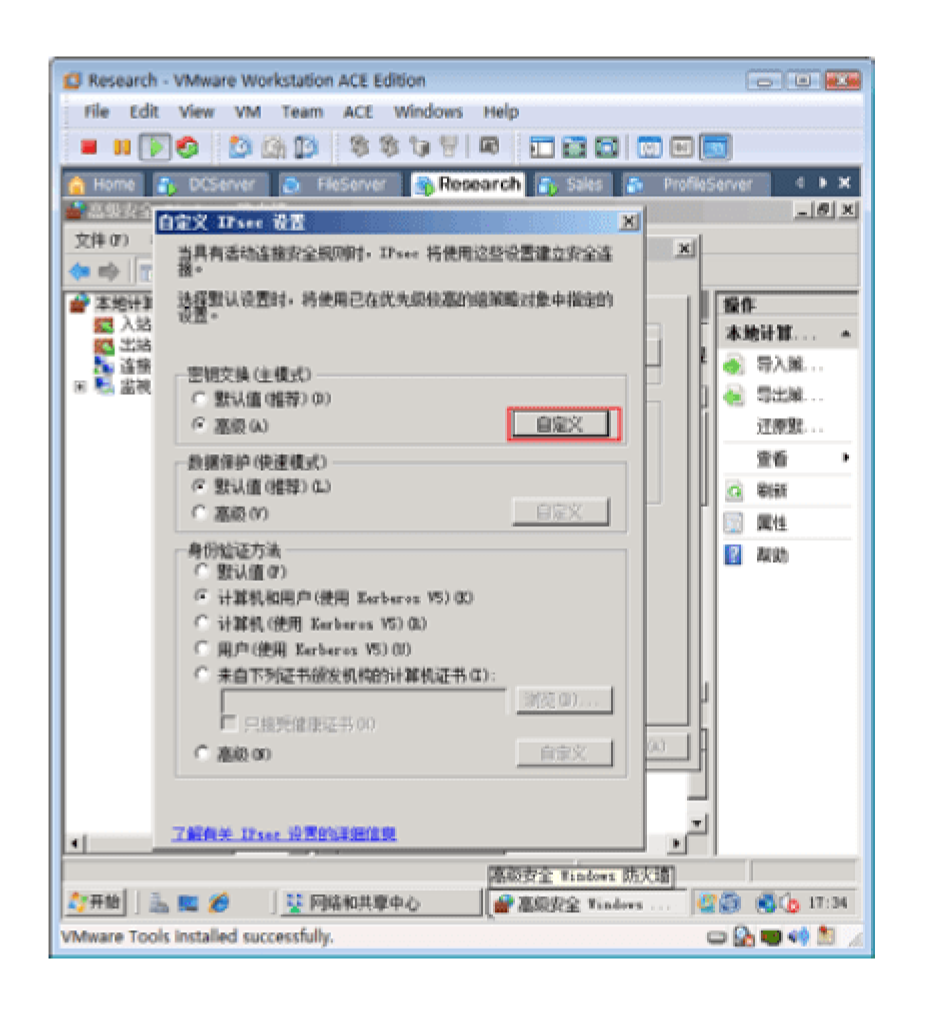



图 9-99　设置密钥交换

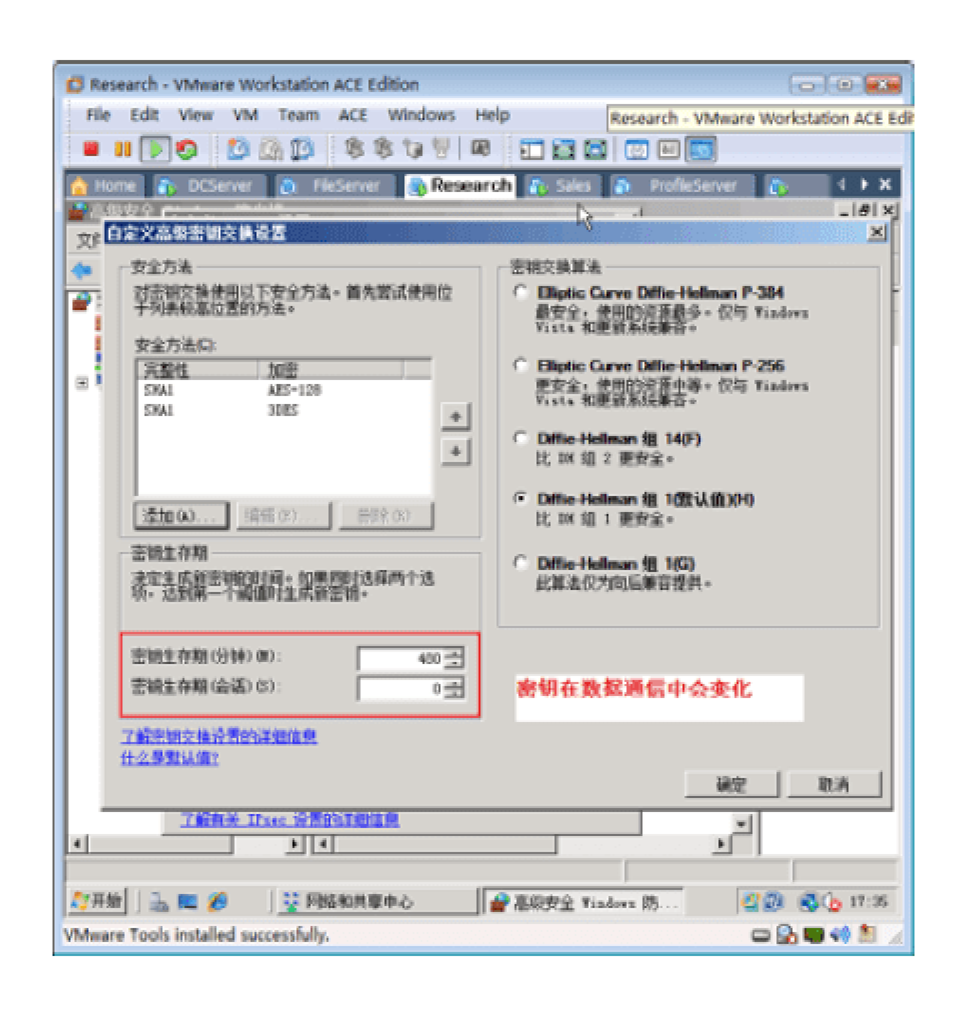


图 9-100　设置密钥生存期

⑤　在图 9-99 所示的“数据保护”选项区域中，选中“高级”单选按钮，单击“自定义”按钮，可以指定完整性和加密算法，如图 9-101 所示。

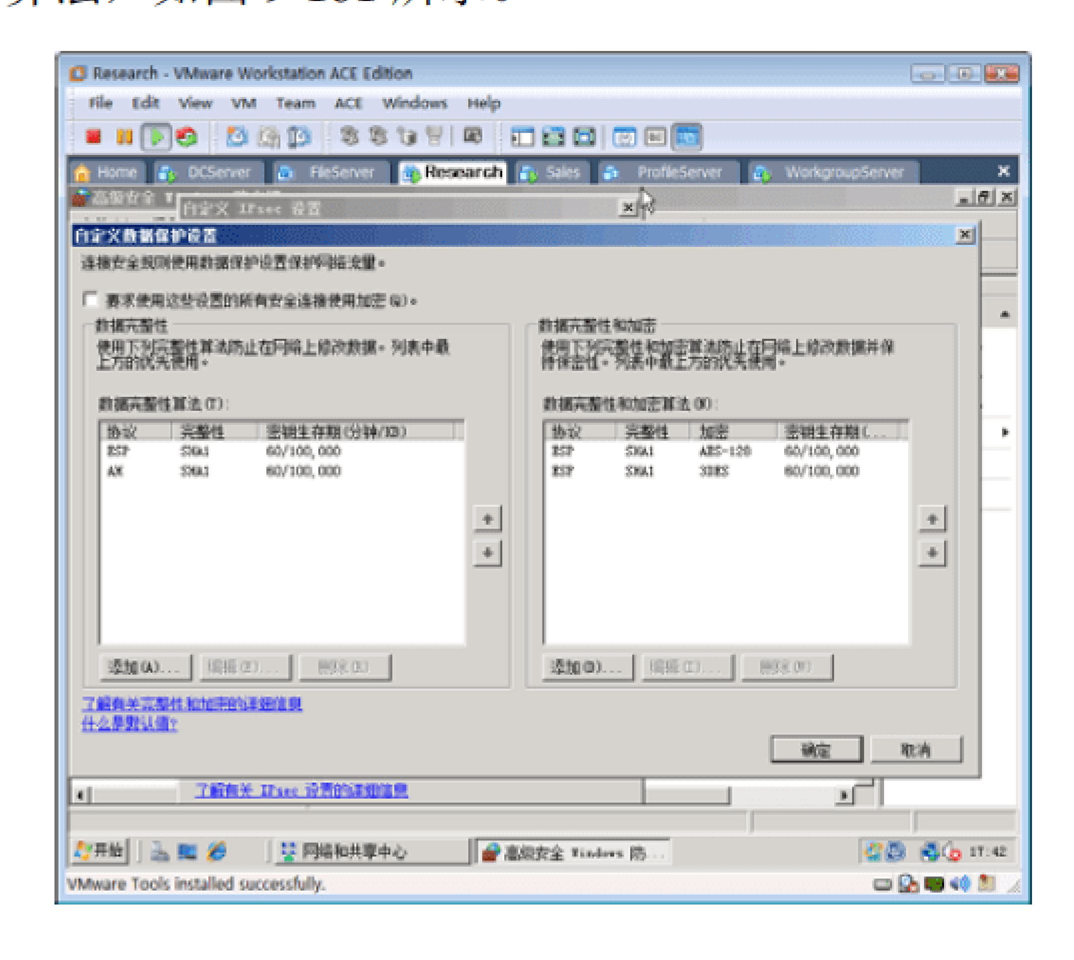


图 9-101　指定完整性和加密算法

9.7　创建软件限制策略

软件限制策略是 Windows XP 和 Windows Server 2003，Windows Server 2008 和 Vista 操作系统中的新功能。软件限制策略提供了一种体制，用于指定允许执行哪些程序以及不允许执行哪些程序。

它们提供了一套策略驱动机制，用于指定允许执行哪些程序以及不允许执行哪些程序。软件限制策略可以帮助组织免遭恶意代码的攻击。也就是说，软件限制策略针对病毒、特洛伊木马和其他类型的恶意代码提供了另一层防护。

虽然软件限制策略是增强计算机安全的重要工具，但它们不能代替其他安全措施，如防病毒程序、防火墙和严格的访问控制列表。

9.7.1 示例：创建软件限制策略

① 如图 9-102 所示，右击“软件限制策略”，在弹出的快捷菜单中选择“创建软件限制策略”命令。

② 如图 9-103 所示，单击“安全级别”选项，可以更改默认的安全级别。此时，可以看到默认安全级别是不受限的。

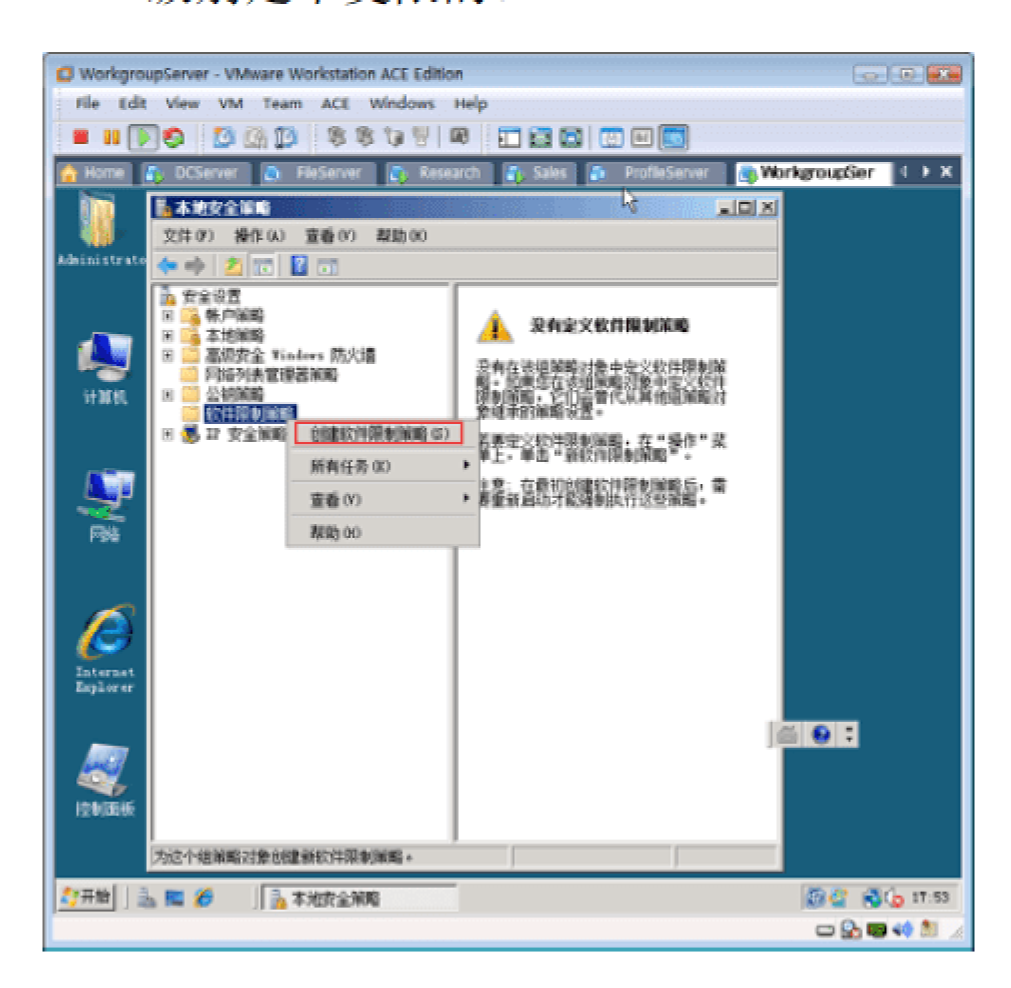


图 9-102 设置软件限制策略

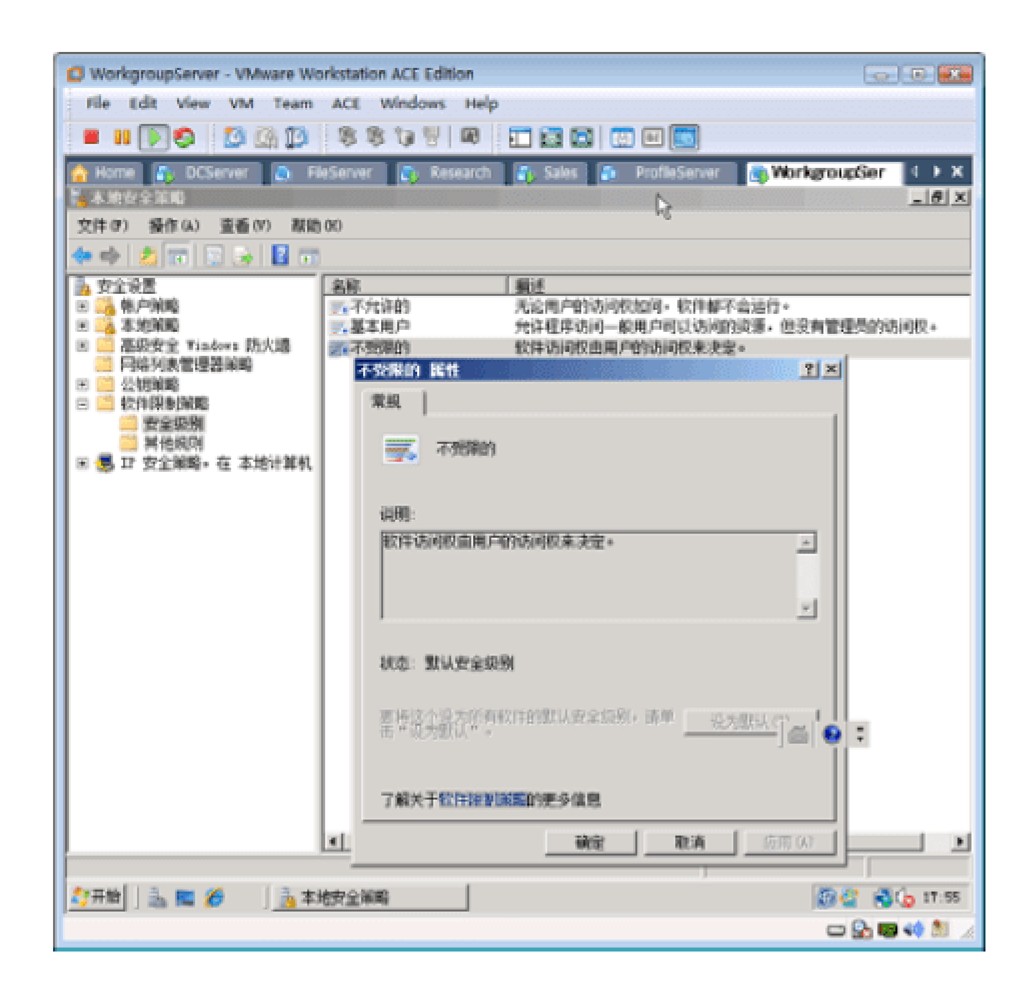


图 9-103 默认不受限

③ 如图 9-104 所示，软件限制策略规则包括证书规则、路径规则、哈希规则及 Internet 区域规则。

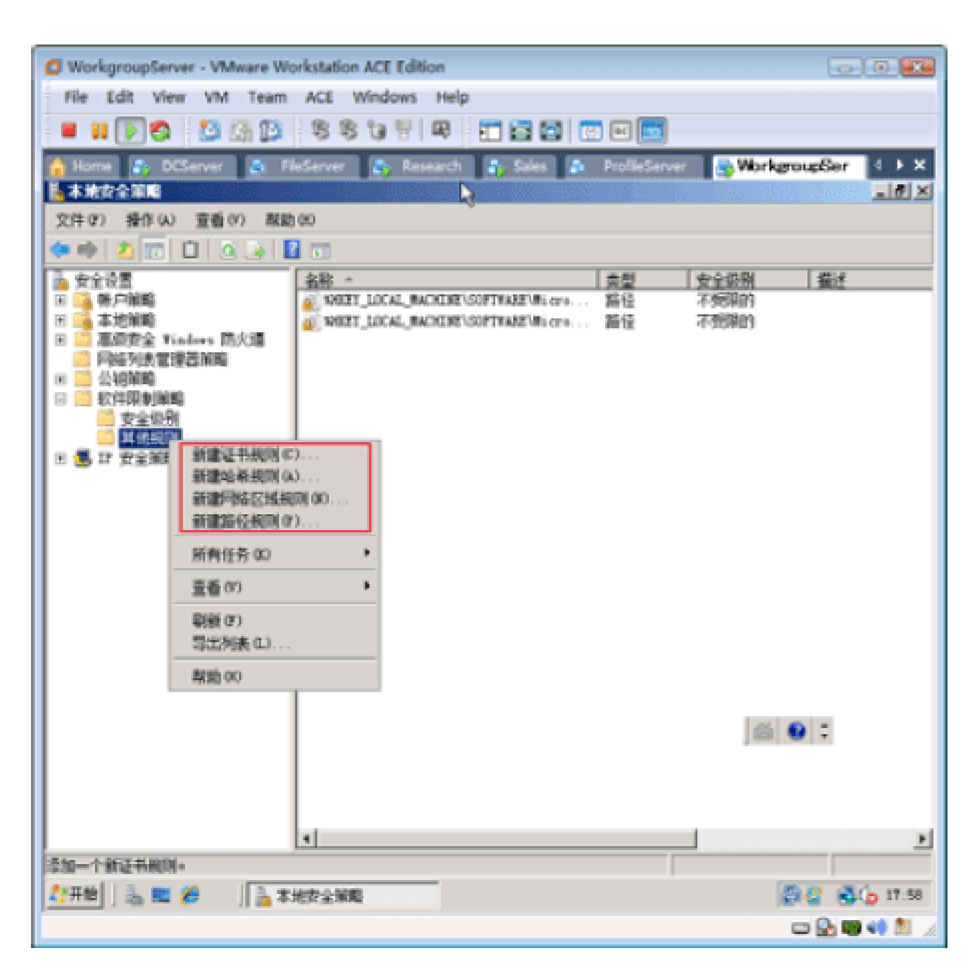


图 9-104 软件限制规则

1. 证书规则

软件限制策略可以通过其签名证书来标识文件。证书规则不能应用到带有 .exe 或 .dll 扩展名的文件，但可以应用到脚本和 Windows 安装程序包。可以创建标识软件的证书，然后根据安全级别的设置，

决定是否允许软件运行。

2. 路径规则

路径规则通过程序的文件路径对其进行标识。由于此规则按路径指定，所以程序发生移动后路径规则将失效。路径规则中可以使用诸如 %programfiles% 或 %systemroot% 之类的环境变量。路径规则也支持通配符，所支持的通配符为 * 和 ?。

3. 哈希(散列)规则

散列是唯一标识程序或文件的一系列定长字节。散列是按散列算法算出来的。软件限制策略可以用 SHA-1(安全散列算法)和 MD5 散列算法根据文件的散列对其进行标识。重命名的文件或移动到其他文件夹的文件将产生同样的散列。

例如，可以创建散列规则并将安全级别设为“不允许的”，以防止用户运行某些文件。文件可以被重命名或移到其他位置并且仍然产生相同的散列。但是，对文件的任何篡改都将更改其散列值并允许其绕过限制。软件限制策略将只识别那些已用软件限制策略计算过的散列。

4. Internet 区域规则

区域规则只适用于 Windows 安装程序包。区域规则可以标识那些来自 Internet Explorer 指定区域的软件。这些区域是 Internet、本地计算机、本地 Intranet、受限站点和可信站点。

9.7.2　指定软件限制策略的软件类型

以上规则所影响的文件类型为“指派的文件类型”中列出的那些类型。系统存在一个由所有规则共享的指定文件类型的列表。如图 9-105 所示，默认情况下列表中的文件类型包括：ADE、ADP、BAS、BAT、CHM、CMD、COM、CPL、CRT、EXE、HLP、HTA、INF、INS、ISP、LNK、MDB、MDE、MSC、MSI、MSP、MST、OCX、PCD、PIF、REG、SCR、SHS、URL、VB 及 WSC。

所以对于正常的非可执行的文件，例如 TXT JPG GIF，这些是不受影响的。如果你认为还有哪些扩展的文件有威胁，也可以将其扩展加入这里；或者你认为哪些扩展无威胁，也可以将其删除。

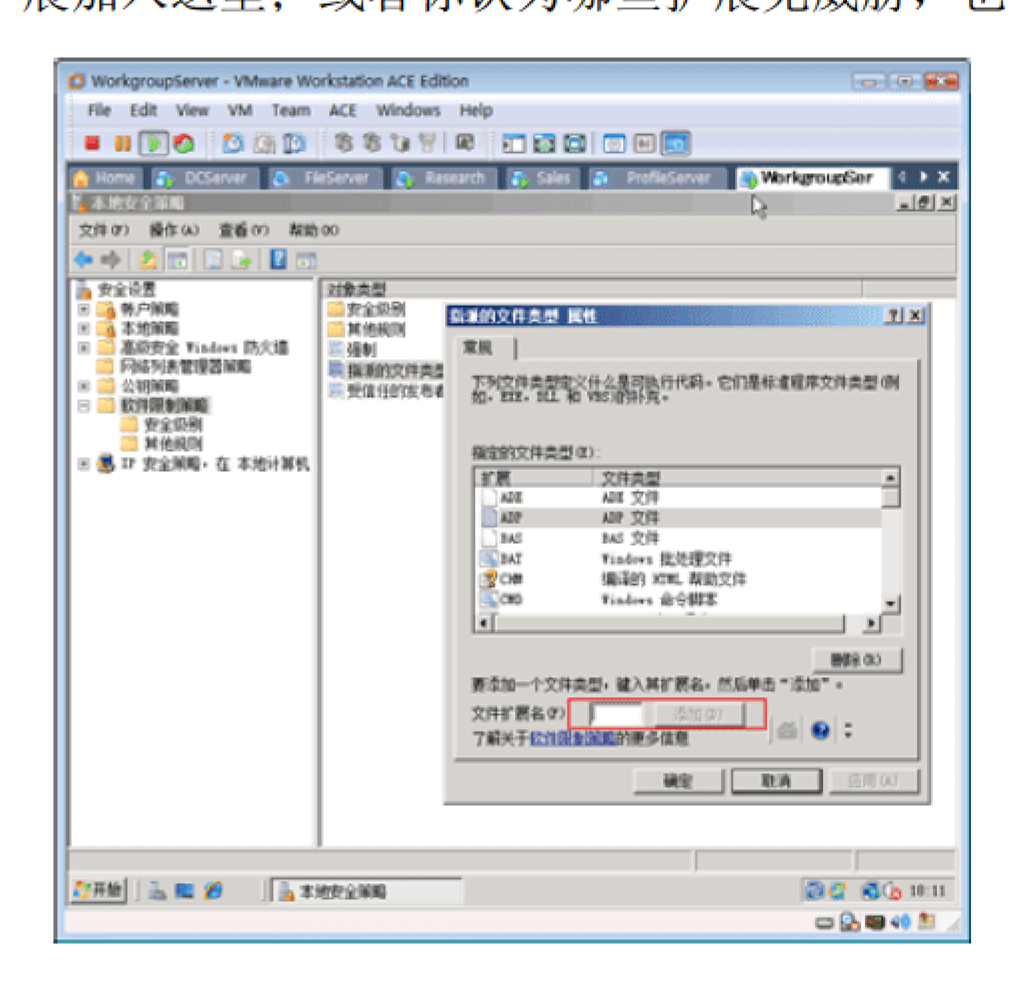


图 9-105　指定软件限制策略扩展名

9.7.3 示例：配置软件限制策略

1. 目标

- 禁止运行计算器软件。
- 禁止 E:\shared 目录下的程序运行。

2. 步骤

① 如图 9-106 所示，选择“开始”→“程序”→“附件”命令，右击“计算器”，在弹出的快捷菜单中选择“属性”命令。

② 如图 9-107 所示，右击“目标”文本框，复制计算器对应的路径。

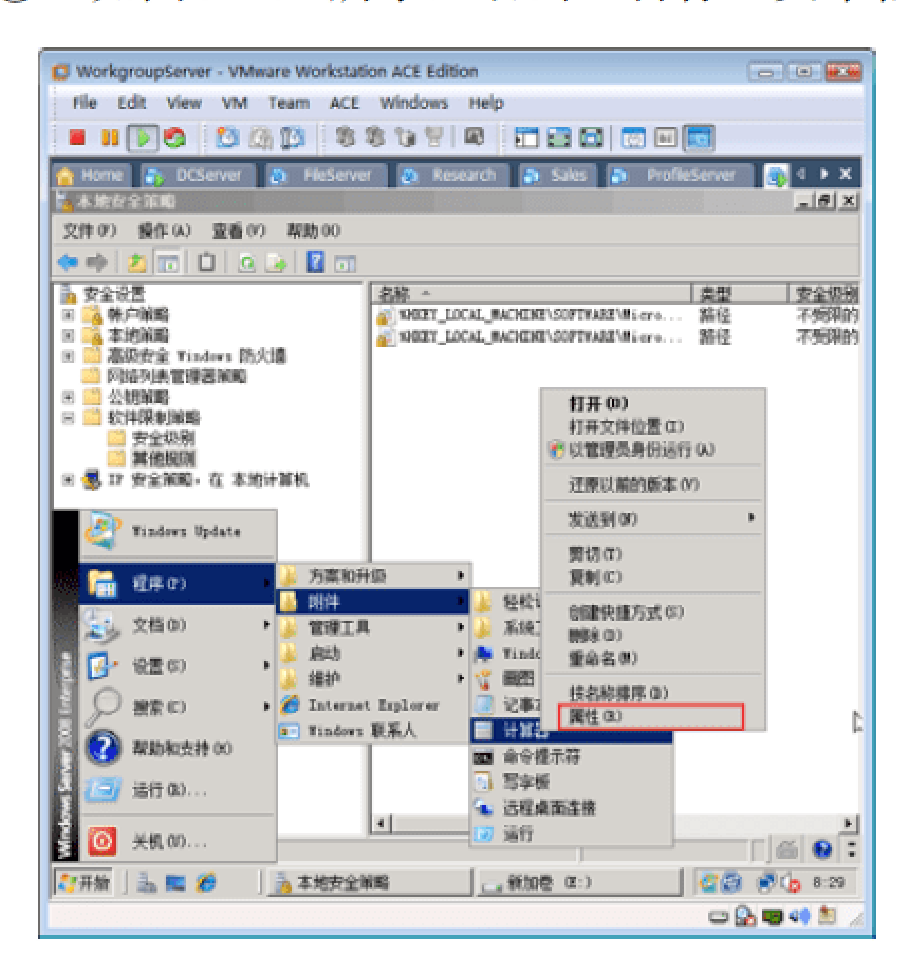


图 9-106 查看计算器属性

图 9-107 复制计算器路径

③ 如图 9-108 所示，右击“其他规则”选项，在弹出的快捷菜单中选择“新建哈希规则”命令。

④ 如图 9-109 所示，在“新建哈希规则”对话框中，单击“浏览”按钮。

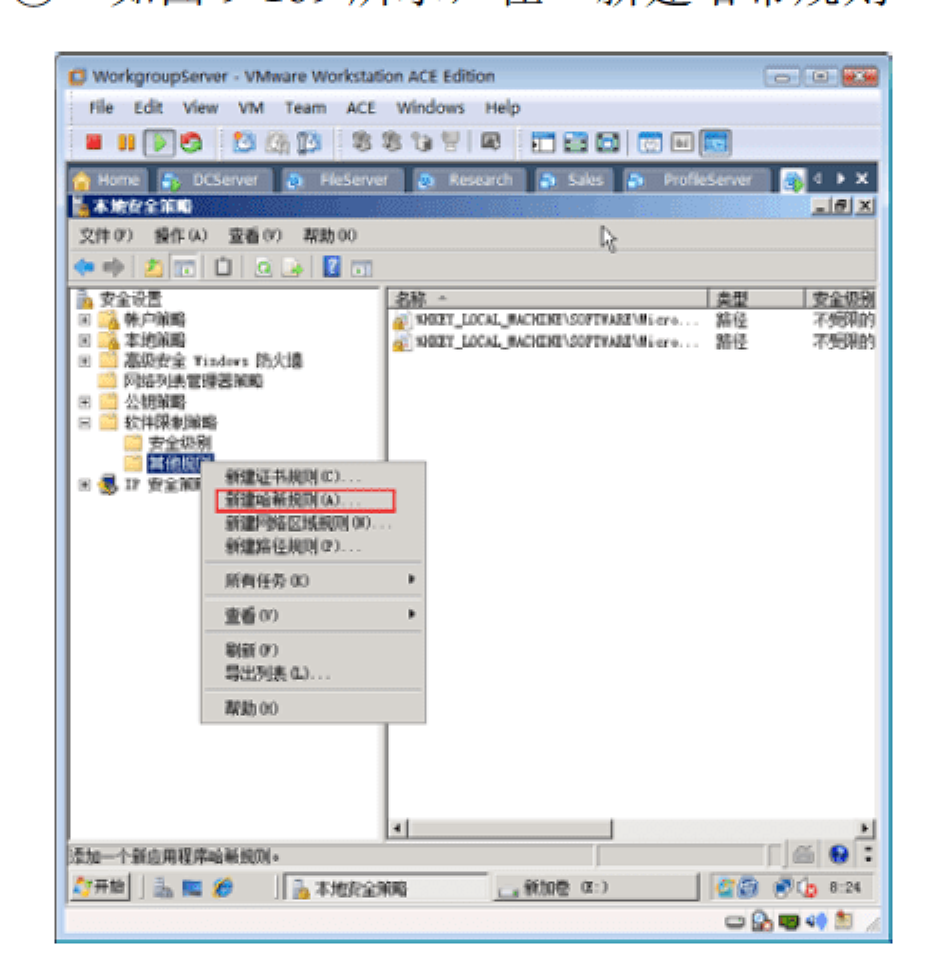


图 9-108 选择新建哈希规则

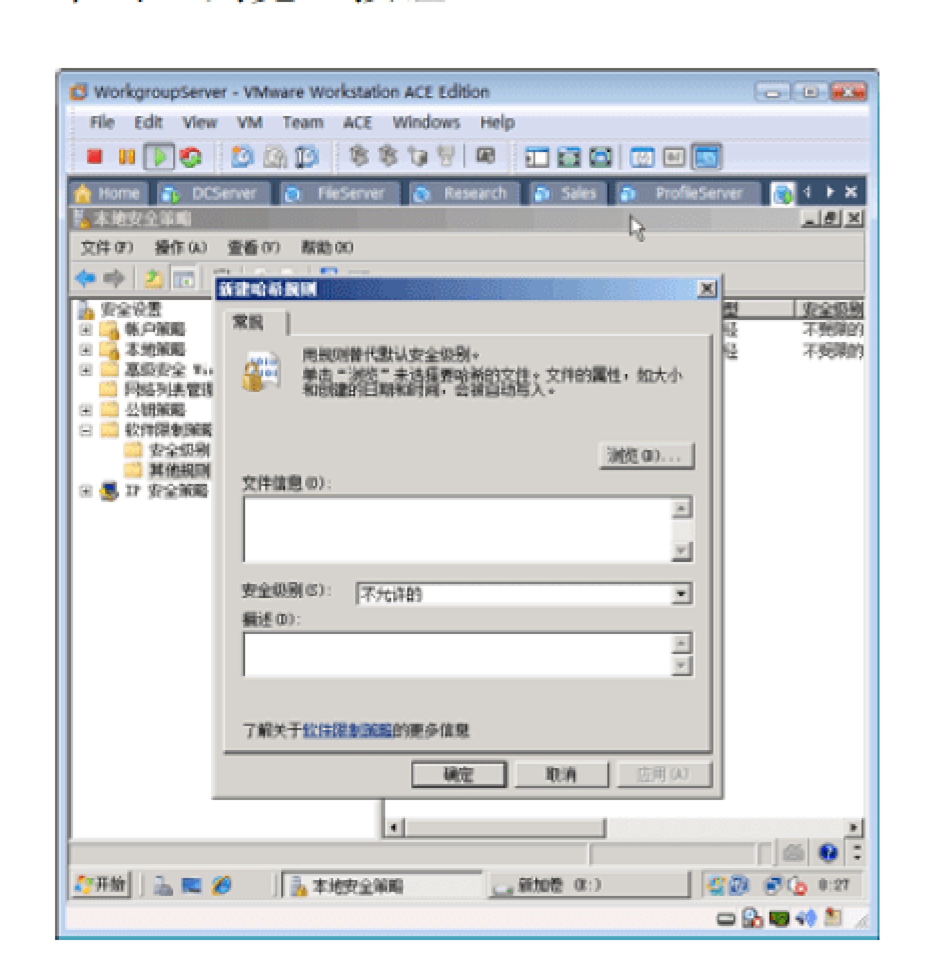


图 9-109 创建新规则

⑤　如图 9-110 所示，在“打开”对话框中，按 Ctrl+V 组合键将刚才复制的计算器的名复制下来，单击“打开”按钮。

⑥　如图 9-111 所示，安全级别设置成“不允许的”，单击“确定”按钮。

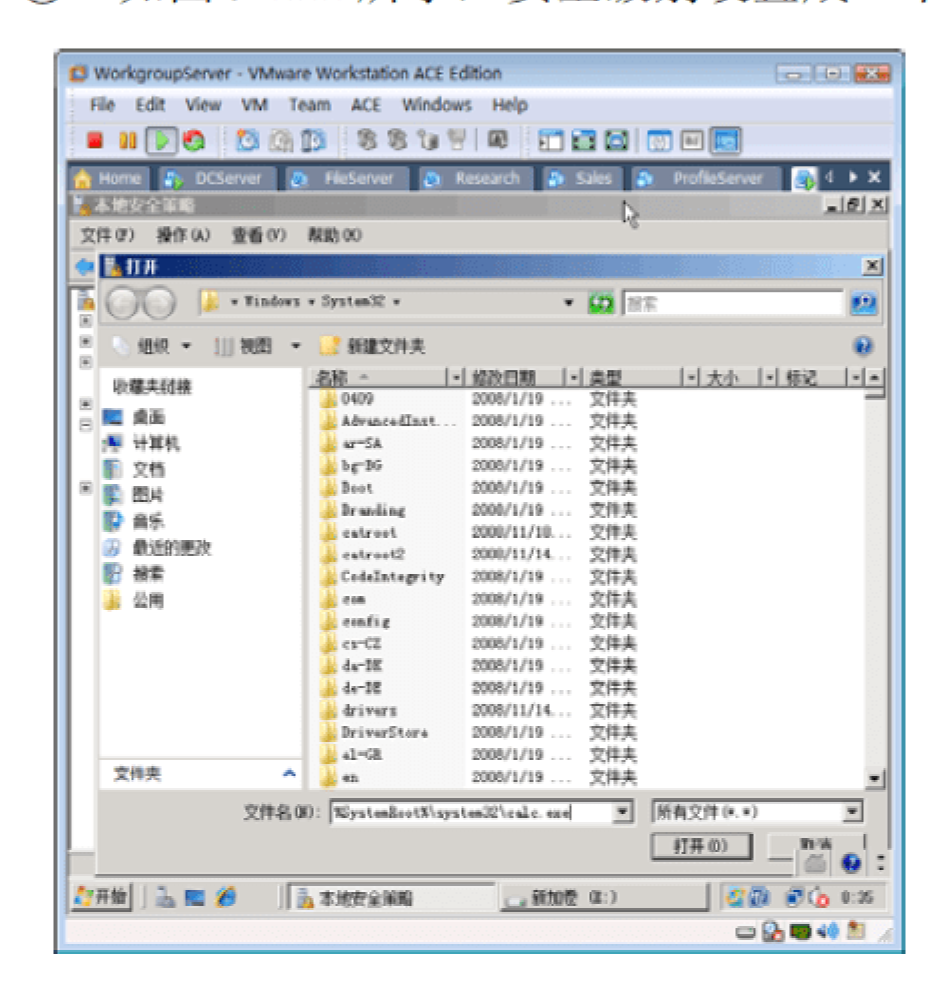


图 9-110　指定程序

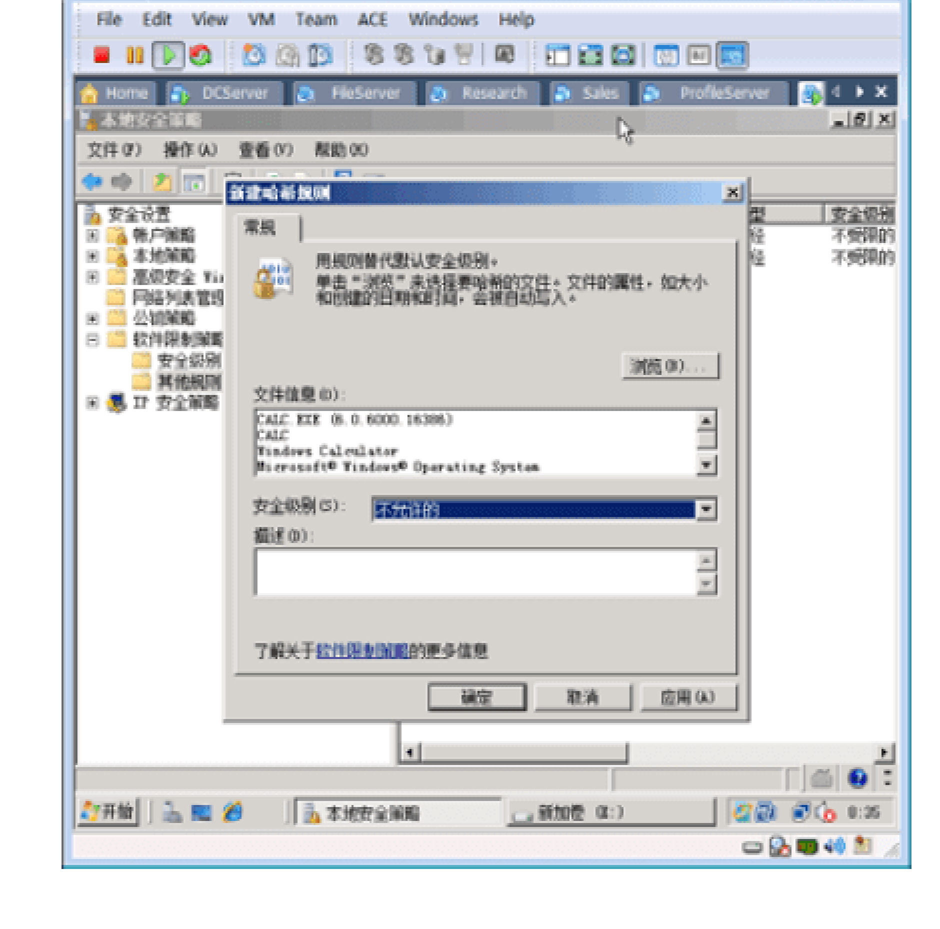


图 9-111　设置安全规则

⑦　如图 9-112 所示，右击“其他规则”选项，在弹出的快捷菜单中选择“新建路径规则”命令。

⑧　如图 9-113 所示，在“新建路径规则”对话框中，输入路径，安全级别选中“不允许的”，单击“确定”按钮。

⑨　重启计算机。软件限制策略重启计算机后生效。

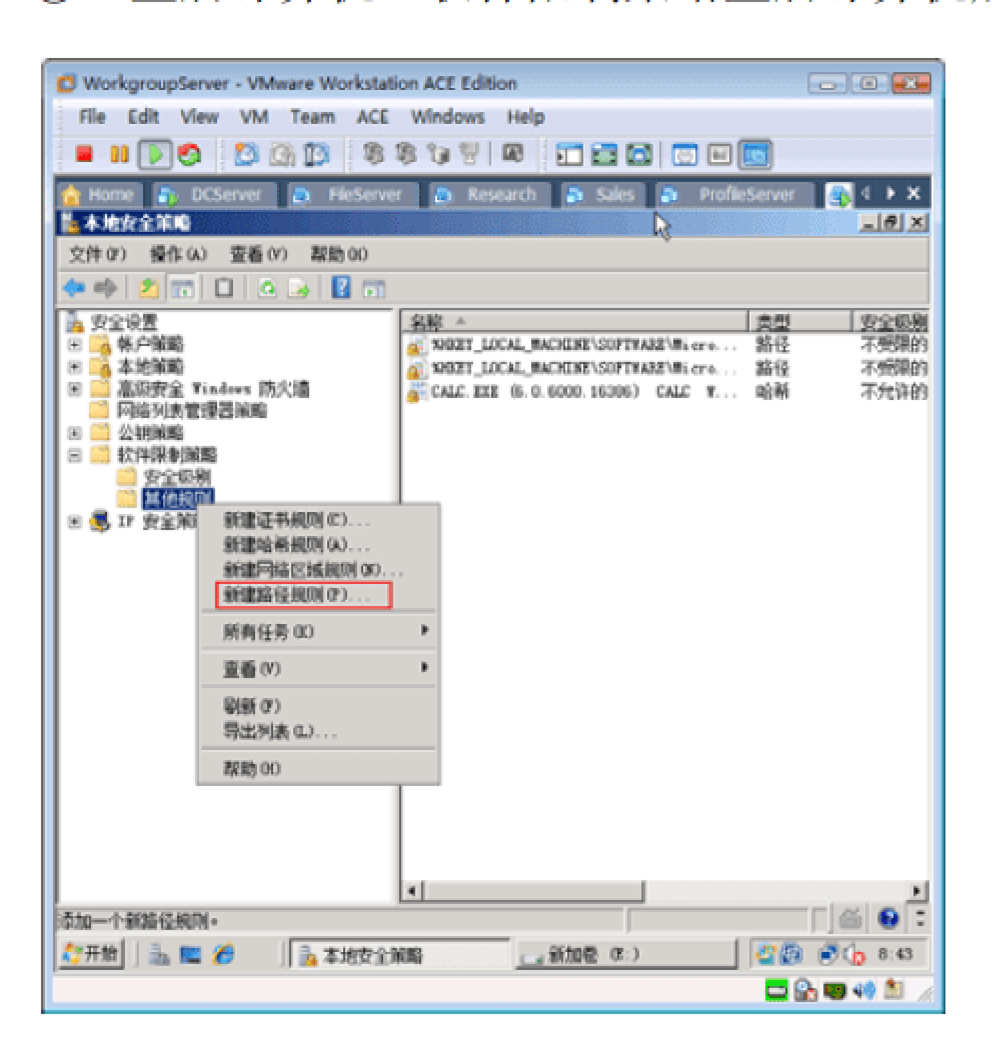


图 9-112　选择新建路径规则

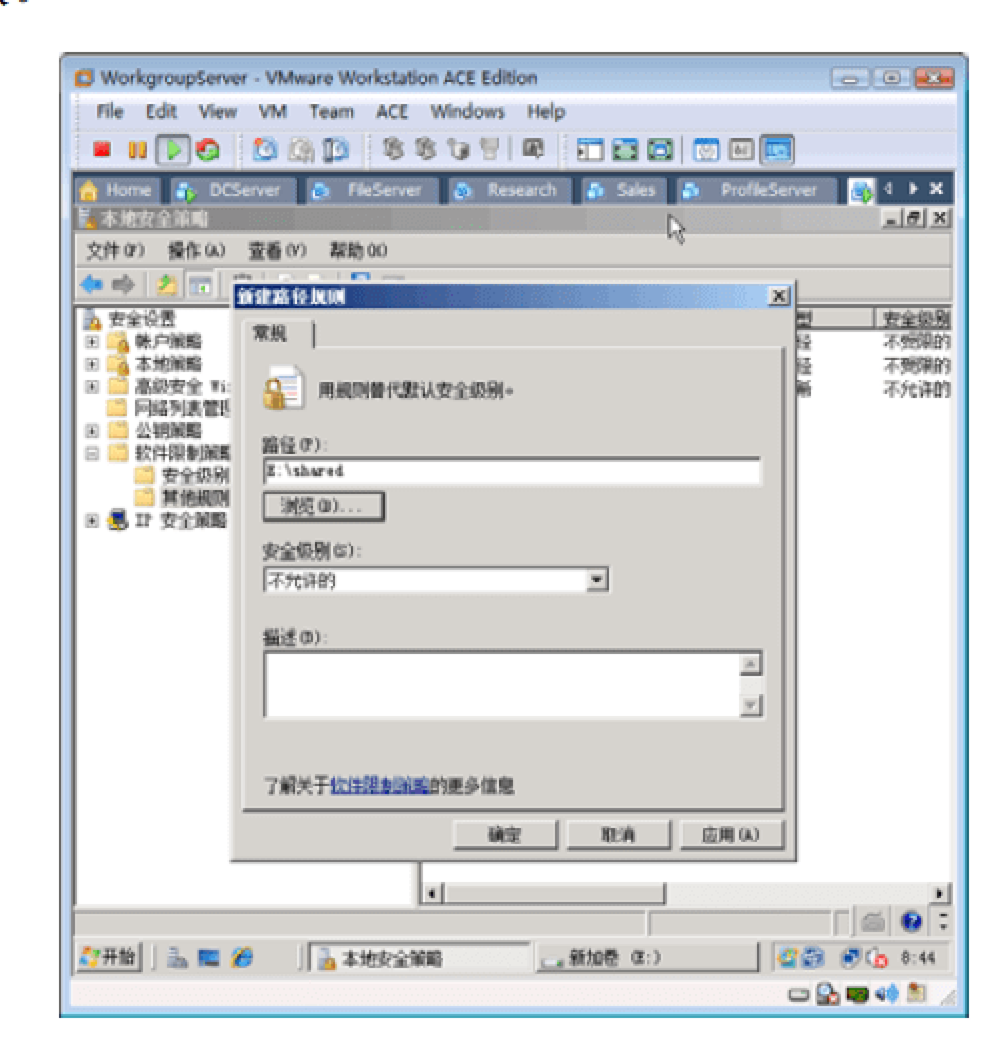


图 9-113　指定路径和规则

⑩　如图 9-114 所示，单击“计算器”软件和 E:\shared 目录下的程序，提示此程序被组策略阻止。



注意：如果程序有多个版本，每个版本的代码都不一样，算出来的哈希值也不一样。使用哈希规则控制程序运行，需要针对同一个程序每个版本配置软件限制策略。

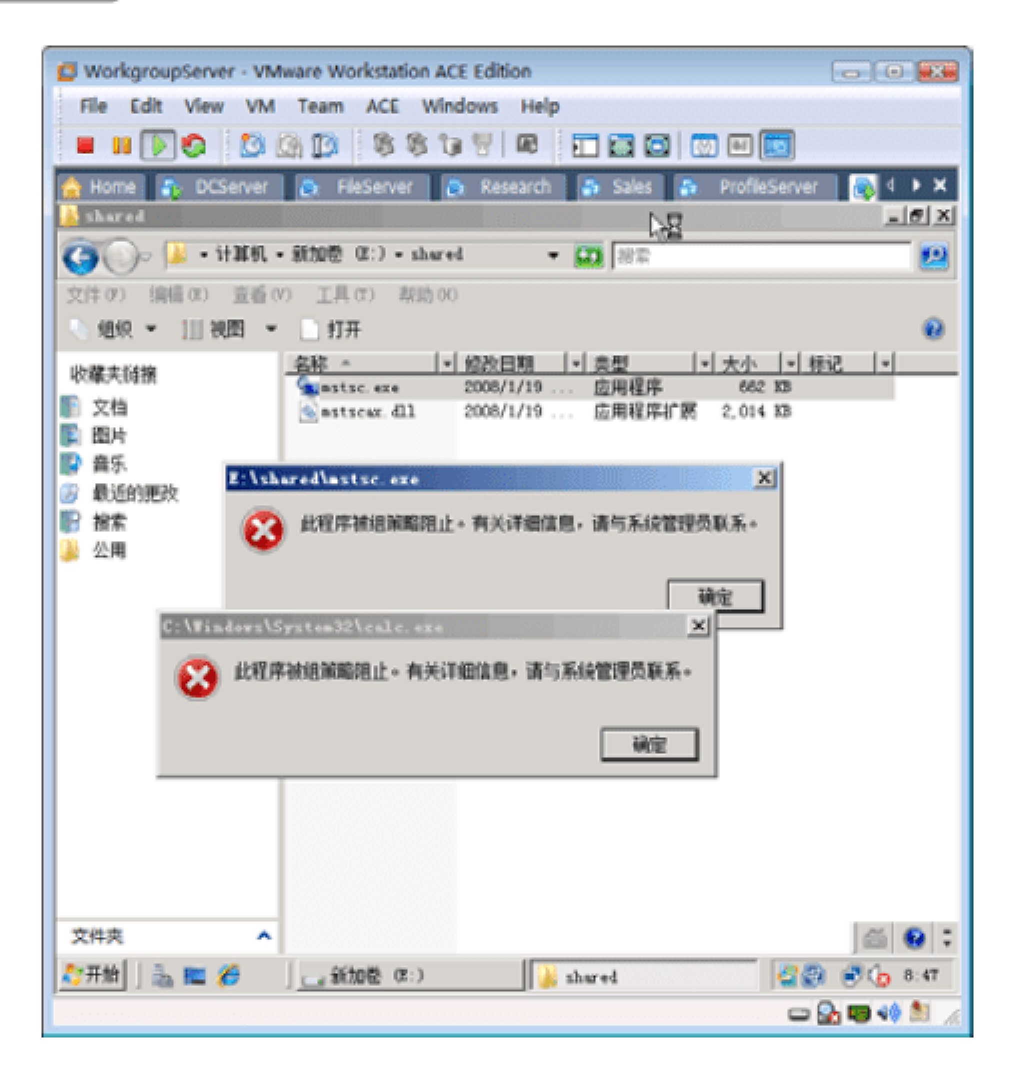


图 9-114　测试软件限制策略

9.7.4　导出导入安全策略

如图 9-115 所示，可以将安全策略导出，在其他计算机上导入。也可以将导出本地安全策略作为策略备份。

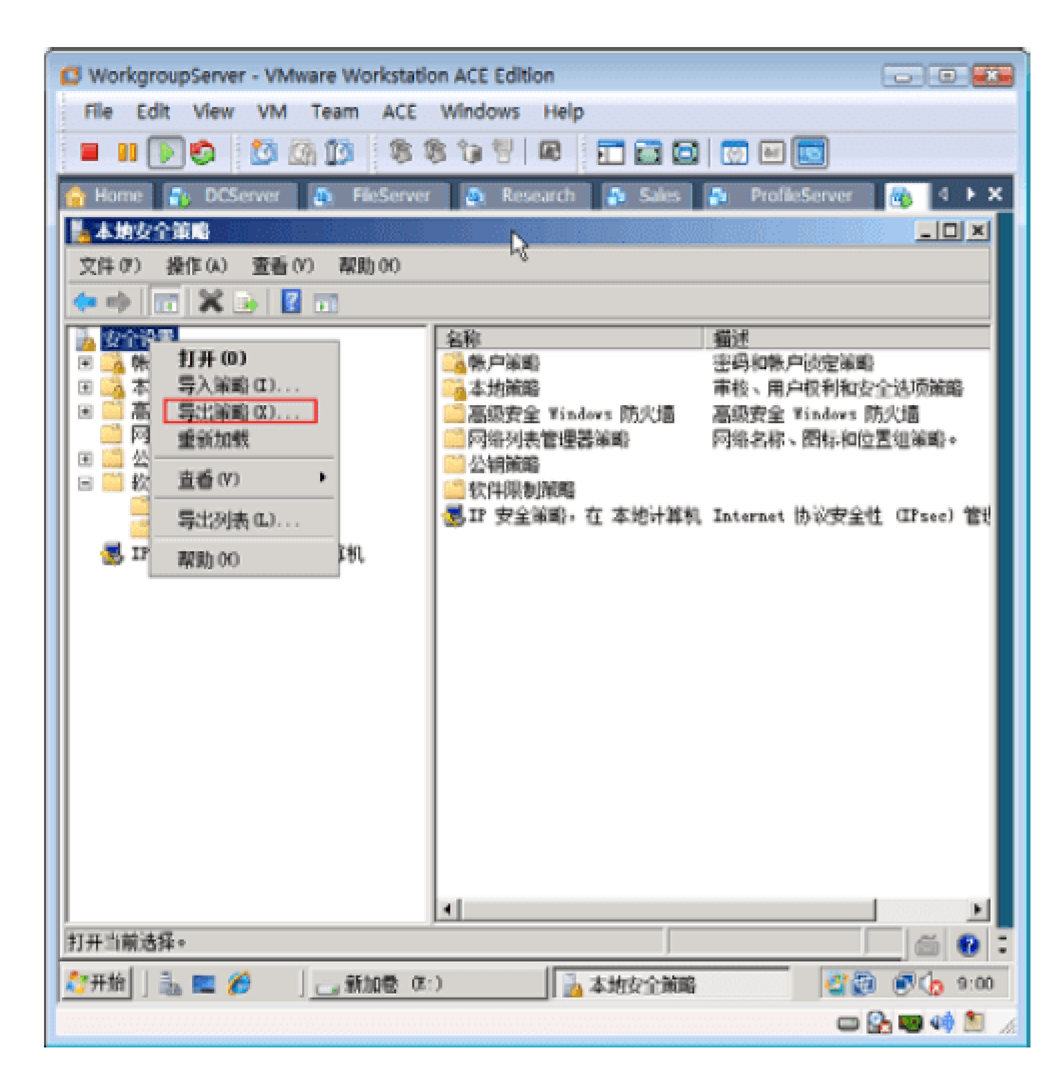


图 9-115　导出导入策略

9.8　使用本地组策略配置系统安全

组策略可以控制计算机和用户的行为。以下将介绍与安全相关的本地组策略设置。本地组策略在 Windows XP、Windows Server 2003、Vista 及 Windows Server 2008 中都可以设置。

9.8.1　关闭自动播放

现在越来越多的病毒利用系统的自动播放功能来进行传播，如果关闭了系统的自动播放，也就相当于掐断了病毒木马的一条传播路径。

① 选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 gpedit.msc，打开本地组策略编辑器。

② 如图 9-116 所示，依次展开“本地计算机策略”→“计算机配置”→“管理模板”→“Windows 组件”→“自动播放策略”节点，双击“关闭自动播放”选项。

③ 在“关闭自动播放 属性”对话框中，选中“已启用”单选按钮，按图 9-116 配置，单击“下一个设置”按钮。

④ 如图 9-117 所示，在出现的“不设置‘始终执行此操作’复选框 属性”对话框中，选中“已启用”单选按钮，单击“下一个设置”按钮。

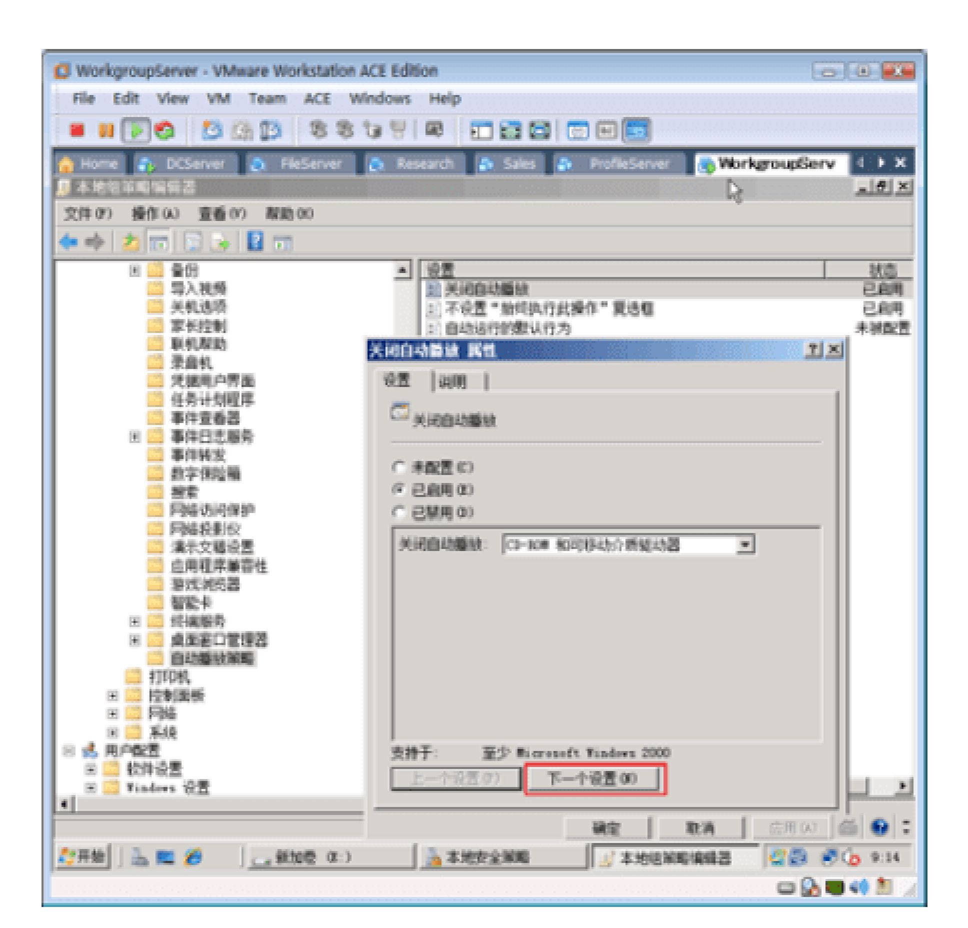


图 9-116　关闭自动播放

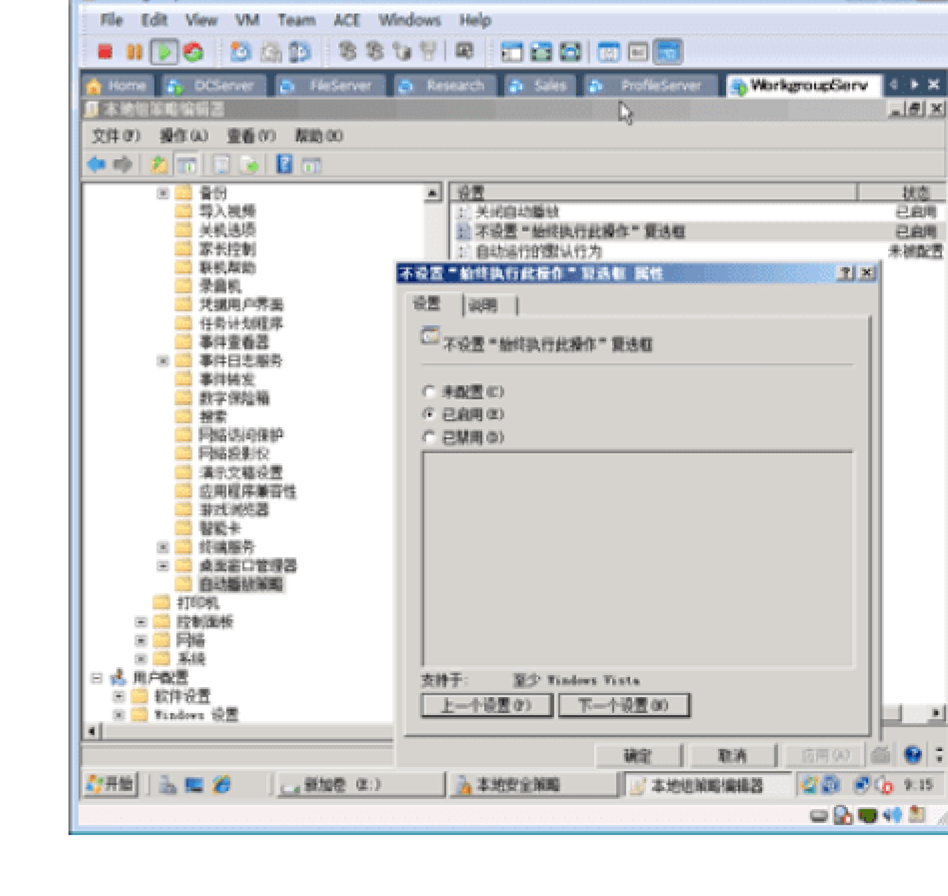


图 9-117　不显示始终执行此操作

⑤ 如图 9-118 所示，自动运行的默认自动运行行为选择“不执行任何自动运行命令”，单击“确定”按钮。

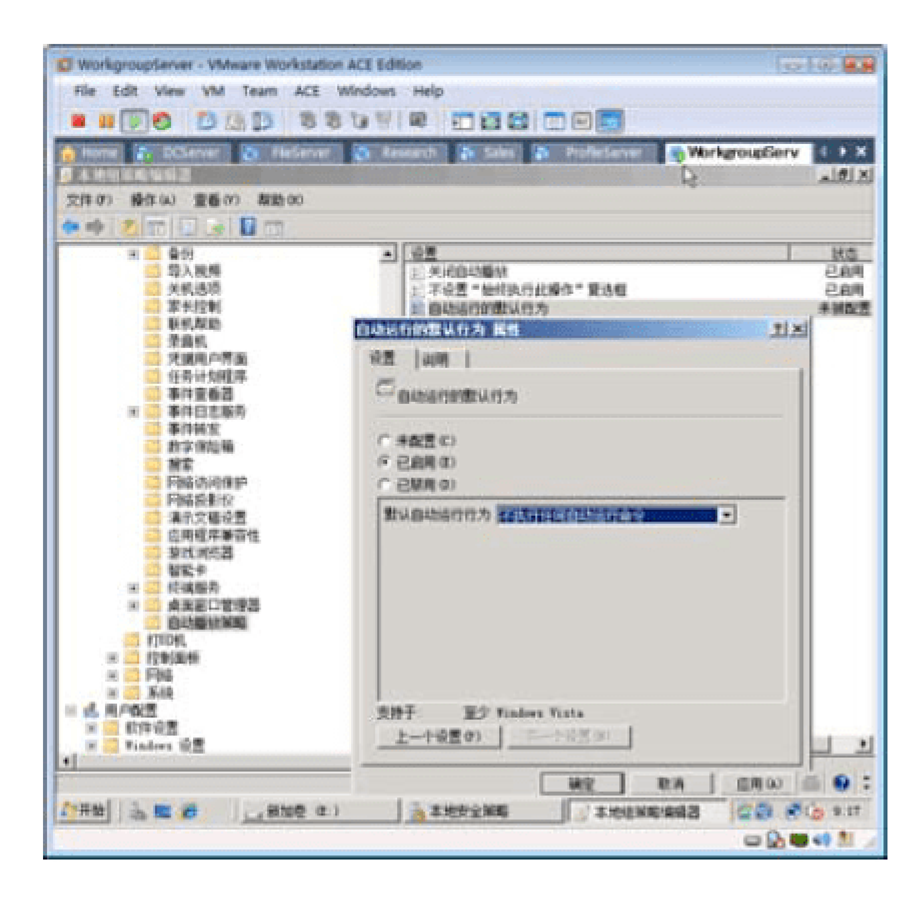


图 9-118　不执行任何自动运行命令

9.8.2 禁止用户使用注册表编辑工具

禁止用户使用注册表编辑工具，能够防止用户更改系统注册表。

① 选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 gpedit.msc，可以打开本地组策略编辑器。

② 如图 9-119 所示，依次展开“本地计算机 策略”→“用户配置”→“管理模板”→“系统”节点，双击“阻止访问注册表编辑工具”选项，选中“已启用”单选按钮，单击“确定”按钮。

③ 如图 9-120 所示，选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 regedit，单击“确定”按钮，提示注册表编辑已被管理员禁用。

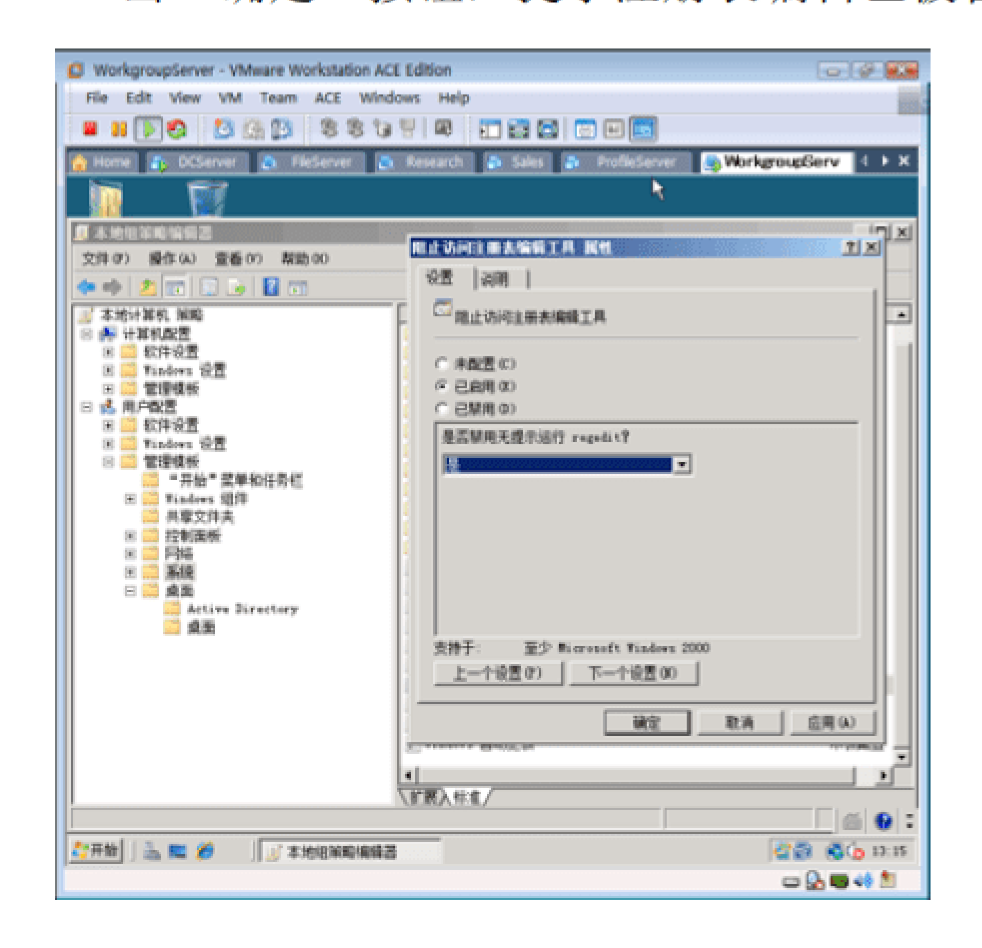


图 9-119 禁止使用注册表编辑工具

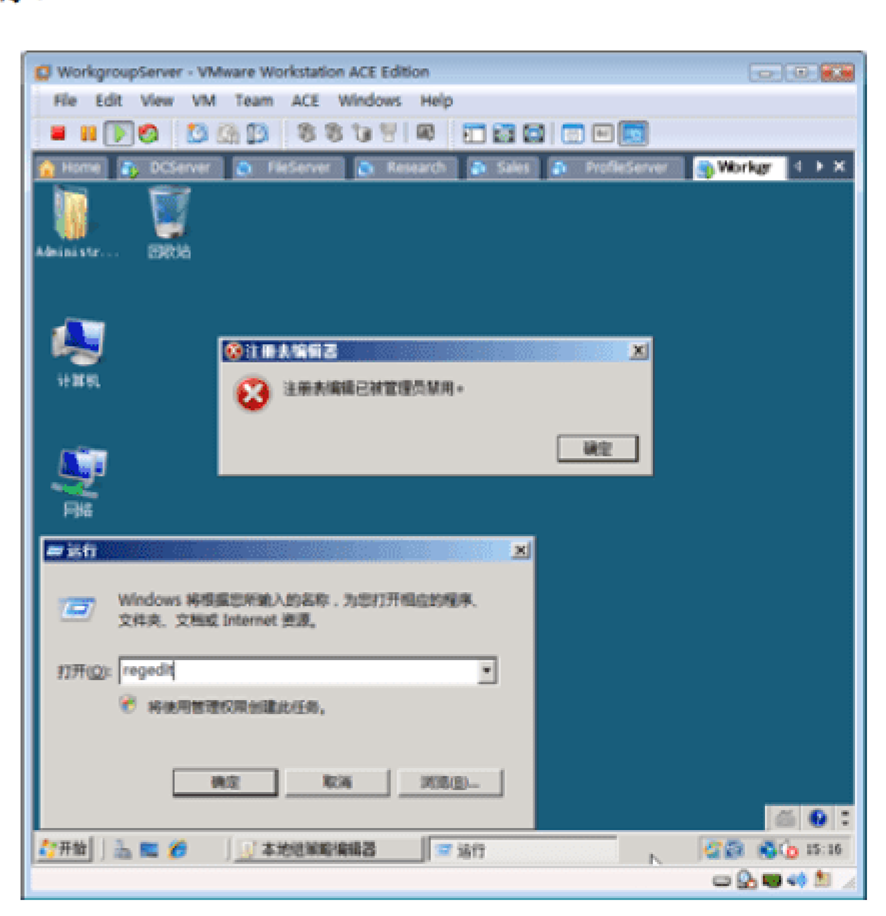


图 9-120 注册表编辑工具被禁用

9.8.3 禁止用户运行特定程序

防止 Windows 运行在此设置中指定的程序。

如果启用此设置，则用户无法运行已添加到不允许的应用程序列表的程序。

此设置仅阻止用户运行由 Windows 资源管理器进程启动的程序。它不会阻止用户运行由系统进程或其他进程启动的程序，如任务管理器。另外，如果允许用户使用命令提示符 (Cmd.exe)，则此设置不会阻止用户在命令窗口中启动不允许他们使用 Windows 资源管理器启动的程序。注意：若要创建不允许的应用程序列表，应依次单击“显示”和“添加”按钮，然后输入应用程序的可执行文件名称(例如，Winword.exe、Poledit.exe 和 Powerpnt.exe)。

如图 9-121 所示，依次展开“本地计算机 策略”→“用户配置”→“管理模板”→“系统”节点，双击“不要运行指定的 Windows 应用程序”选项，选中“已启用”单选按钮，依次单击“显示”和“添加”按钮，然后输入 mspaint.exe，单击“确定”按钮。



注意：此设置只是根据程序的名称进行限制，如果用户更改应用程序的名称，此设置将不能控制此应用程序。

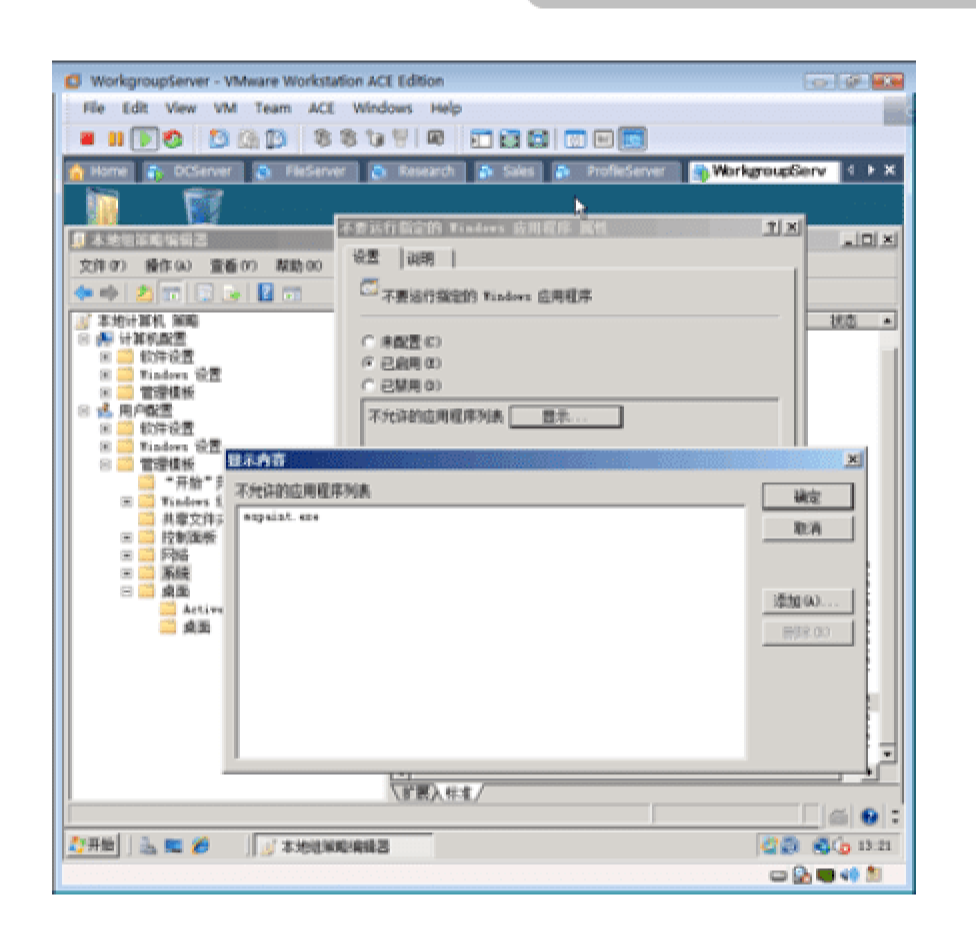


图 9-121　禁止用户运行特定程序

9.8.4　禁止恶意程序“不请自来”

在 Windows Server 2008 系统环境中使用 IE 浏览器上网浏览网页内容时，时常会有一些恶意程序不请自来，偷偷下载保存到本地计算机硬盘中，这样不但会白白浪费宝贵的硬盘空间资源，而且也会给本地计算机系统的安全带来不少麻烦。为了让 Windows Server 2008 系统更加安全，往往需要借助专业的软件工具才能禁止应用程序随意下载，很显然，这样操作不但麻烦而且比较累人。其实，在 Windows Server 2008 系统环境中，只需简单地设置一下系统组策略参数，就能禁止恶意程序自动下载保存到本地计算机硬盘中了，下面就是具体的设置步骤。

① 以特权账号进入 Windows Server 2008 系统环境，选择“开始”→“运行”命令，在系统“运行”文本框中执行 gpedit.msc 命令，打开本地计算机的组策略编辑窗口。

② 如图 9-122 所示，在组策略编辑窗口左侧区域展开“计算机配置”→“管理模板”→“Windows 组件”→Internet Explorer→“安全功能”→“限制文件下载”节点，双击“限制文件下载”子项下面的“Internet Explorer 进程”组策略选项，在其属性设置窗口中，选中“已启用”单选按钮，再单击“确定”按钮，退出组策略属性设置窗口。

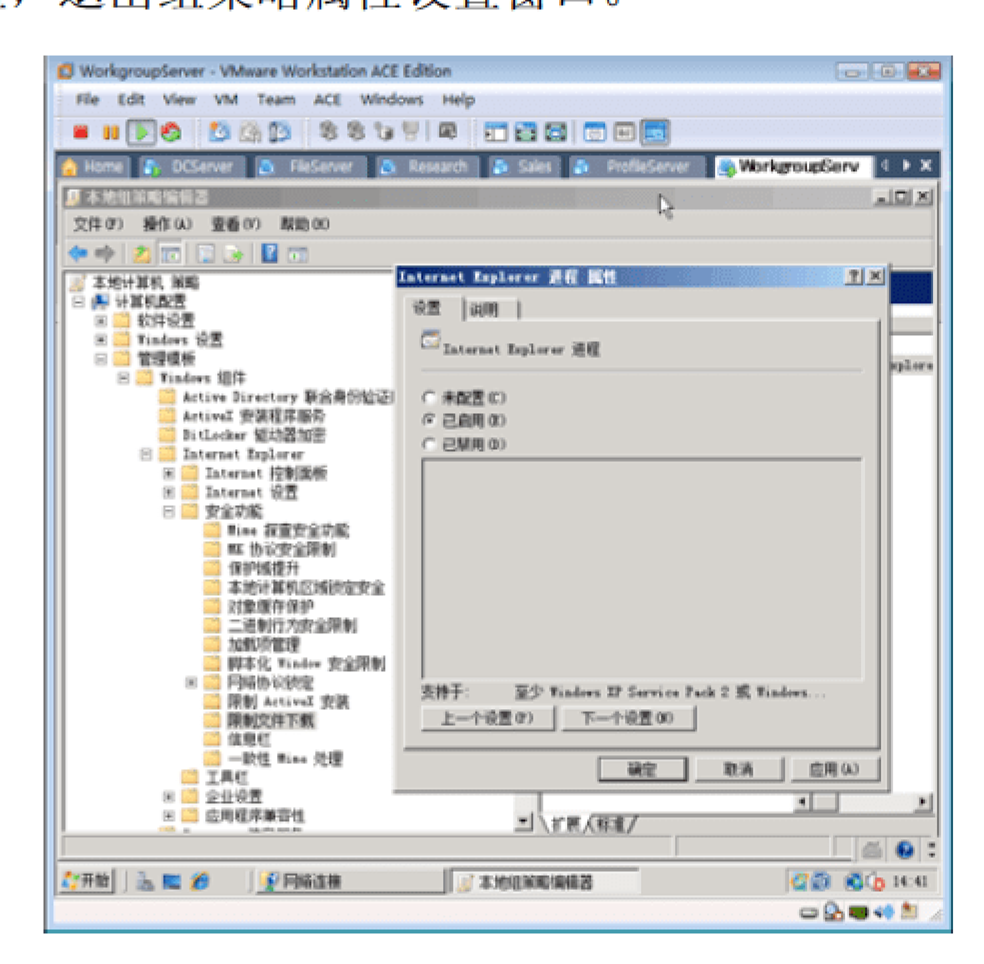


图 9-122　限制文件下载

这样一来，我们就能成功启用限制 Internet Explorer 进程下载文件的策略设置，日后 Windows Server 2008 系统就会自动弹出阻止 Internet Explorer 进程的非用户初始化的文件下载提示，单击提示对话框中的“确定”按钮，恶意程序就不会通过 IE 浏览器窗口随意下载保存到本地计算机硬盘中了。

9.8.5 跟踪用户登录情况

一般情况下，用户对自己的计算机使用情况都比较熟悉，比如你会记得上一次登录系统的大概时间。如果用户还能让 Windows Server 2008 记录下登录信息，然后在每次登录系统时，将前后两次的时间比较一下，如果发现时间不一致，这就说明有人曾经试图非法登录你的账户。

此策略设置控制系统是否向用户显示有关以前的登录和登录失败次数的信息。

对于 Windows Server 2008 功能级别域中的本地用户账户和域用户账户，如果启用了此设置，将在该用户登录后出现一则消息，显示该用户上次成功登录的日期和时间、该用户名上次尝试登录而未成功的日期和时间以及自该用户上次成功登录以来未成功登录的次数。用户必须确认该消息，然后才能登录到 Microsoft Windows 桌面。

① 选择“开始”→“运行”命令，在打开的“运行”对话框中，输入 gpedit.msc，打开组策略编辑器。

② 依次展开“计算机配置”→“管理模板”→“Windows 组件”→“Windows 登录选项”节点，然后在右侧窗格中双击“在用户登录期间显示有关以前登录的信息”，然后在弹出的对话框中选中“已启用”单选按钮，最后单击“确定”按钮，如图 9-123 所示。

③ 注销，以管理员的账户登录，输入一次错误的密码，然后输入正确的密码，将会出现登录不成功的信息，如图 9-124 所示。

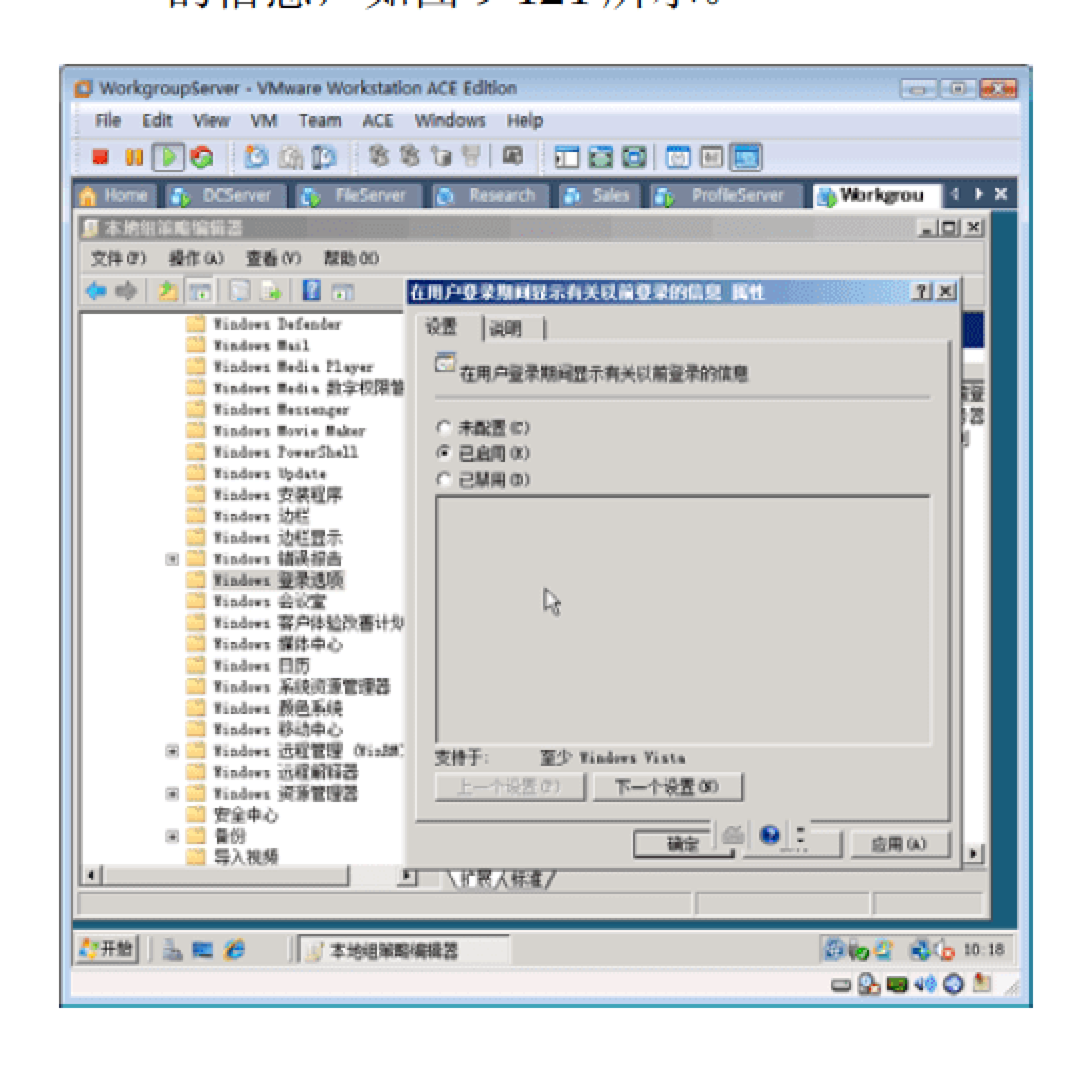


图 9-123 设置显示以前登录信息

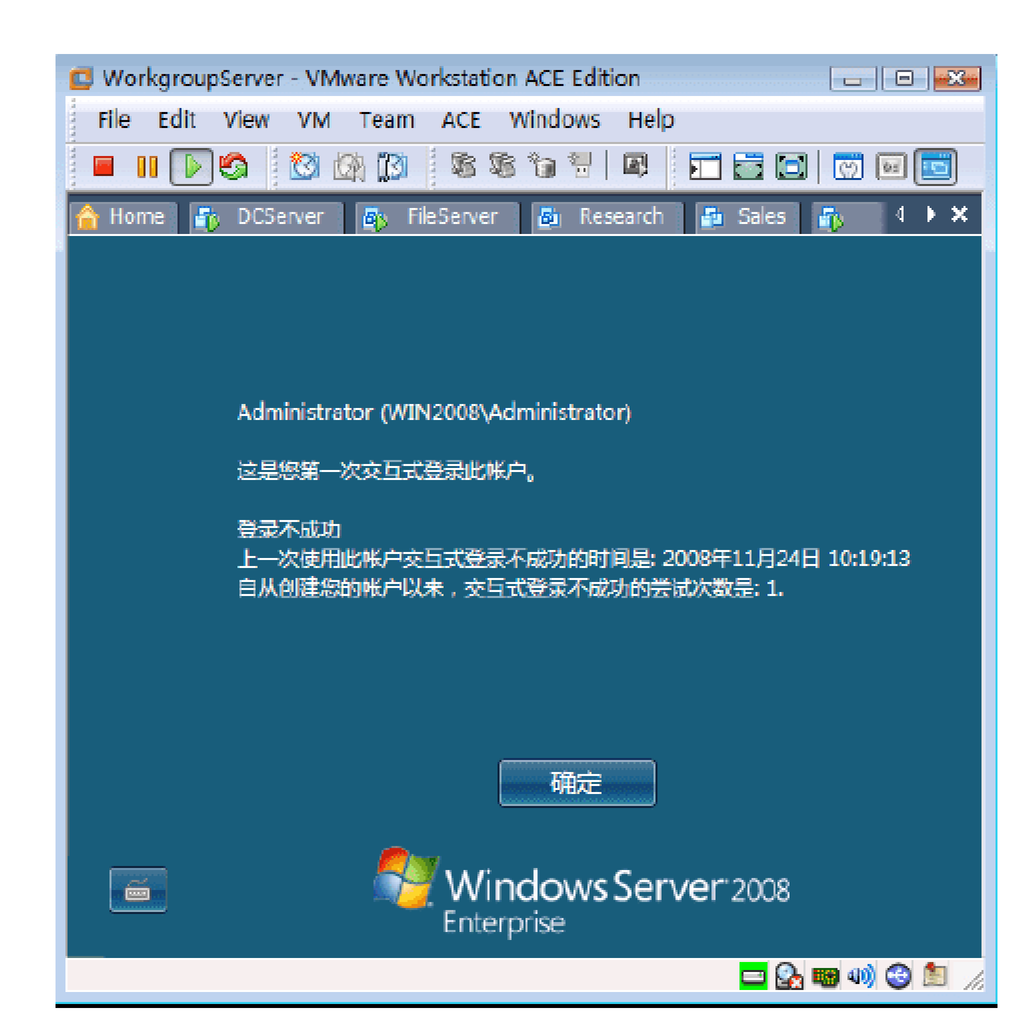


图 9-124 显示以前登录的信息

第 10 章　配置打印功能

本章将重点介绍如何实现部署打印机与管理打印服务器。

在域环境中部署打印机，这样域用户登录后，就能自动连接到该部门使用的打印机。配置 Internet 打印机，即远程用户使用 TCP 的 80 端口将打印作业发送到公司服务器，这样可以穿透大多数防火墙。在 Windows Server Core 上安装打印服务角色，使用图形界面管理 Windows Server Core 上的打印机。

关键词

- 理解打印过程
- 掌握如何安装共享打印机
- 设置打印机属性
- 掌握如何管理打印机访问
- 使用组策略部署打印机
- 发布打印机到活动目录
- 掌握如何设置打印机优先权
- 掌握如何计划打印机的可用性
- 掌握如何配置打印池
- 配置 Internet 打印
- 配置 Windows Server core 作为打印服务器

10.1 Windows Server 2008 打印概述

- 用户使用 Windows Server 2008 家族中的产品，可以在整个网络范围内共享打印资源。各种计算机和操作系统上的客户端，可以通过 Internet 将打印作业发送到运行 Windows Server 2008 家族操作系统的打印服务器所连接的本地打印机，或者发送到使用内置或外置网卡连接到网络或其他服务器的打印机。
- Windows Server 2008 家族中的产品支持多种高级打印功能。例如，无论运行 Windows Server 2008 家族操作系统的打印服务器计算机位于网络中的哪个位置，管理员都可以对它进行管理。另一项高级功能是，客户不必在 Windows XP 客户端计算机上安装打印机驱动程序就可以使用打印机。当客户端连接运行 Windows Server 2008 家族操作系统的打印服务器计算机时，驱动程序将自动下载。
- Windows Server 2008 家族中的产品使得管理员更加容易在一个中心位置安装网路打印机和配置打印资源。客户可以配置运行 Microsoft Windows 95、Microsoft Windows 98 或 Microsoft Windows NT 操作系统的客户端计算机来访问网络打印设备，以实现打印。
- Windows Server 2008 家族的打印增强特性有以下几点。
    - 打印设置。
    - 在群集的所有节点上安装打印机驱动程序。
    - 打印管理。
    - 打印机文件夹。
    - Internet 打印。
    - 目录服务。
    - 标准端口监视器。
    - 打印队列监视。

打印服务器就是专门管理网络打印机的计算机，打印服务器可以是网络上的任何一台计算机。如果用户添加一台通过网络适配器直接连接到网络的打印机，则可以采用以下两种方法打印。

1. 方法一

不使用打印服务器，而直接将打印机添加到每个用户的计算机上。

使用条件如下：一个小型工作组网络仅有几台计算机和一台直接与网络相连的打印机。网络上的用户不共享该打印机，每个用户都将打印机添加到自己的 Printers and Faxes 文件夹中，并设置各自的驱动程序。

该配置的缺点如下。

- 用户不知道打印机的真实状态，每台计算机的打印队列都只显示各自发送的打印作业，用户不能确定自己的打印作业相对于其他计算机发送的所有打印作业的位置。
- 卡纸或纸盒无纸等错误消息只显示在当前打印作业所在的队列上。
- 对提交打印文档的所有处理任务都在这一台计算机上完成。

2. 方法二

先将打印机添加到打印服务器上，然后通过打印服务器将每个用户连接到打印机。让一台运行 Windows Server 2008 家族操作系统的计算机充当打印服务器，该计算机将添加打印机，并与其他用户共

享打印机。

使用打印服务器打印具有如下优点。

- 打印服务器可以管理打印机驱动程序设置。
- 在连接打印机的每台计算机上都会显示一个完整的打印队列，每个用户都能看见自己的打印作业相对于其他等待打印的打印作业的位置。
- 由于错误信息会出现在所有计算机上，每个用户都能了解打印机的真实状态。
- 某些处理任务可以从客户端计算机转移到打印服务器上进行。
- 可有一个日志，供要审核打印机事件的管理员查阅。

使用打印服务器的唯一缺点在于，它需要一台计算机来充当打印服务器。但是，它并不需要一台专用计算机；通常，打印服务器由同时执行其他任务的服务器担任。

10.2 实战：在企业配置和管理打印

任务描述

在企业环境中配置和管理打印机。

- DCServer 作为域控制器和 DNS 服务器，服务器 FileServer 作为打印服务器， Sales 是销售部门的计算机。
- ProfileServer 作为研发部门的打印服务器。
- WangRS 是销售部门经理，在 Sales 计算机办公，使用 FileServer 打印服务器打印日常文档。
- ZhangJC 是销售部门员工，也使用 FileServer 打印服务器打印日常文档。
- WangBH 是销售部门的驻外员工，销售部经理关注销售情况，每周需要将销售报告使用企业内部的 FileServer 打印服务器打印出来。
- 销售人员经常带着 Sales 笔记本出差在外地，需要通过 Internet 打印将打印作业发送到打印服务器 FileServer。

实战环境

实战环境如图 10-1 所示。

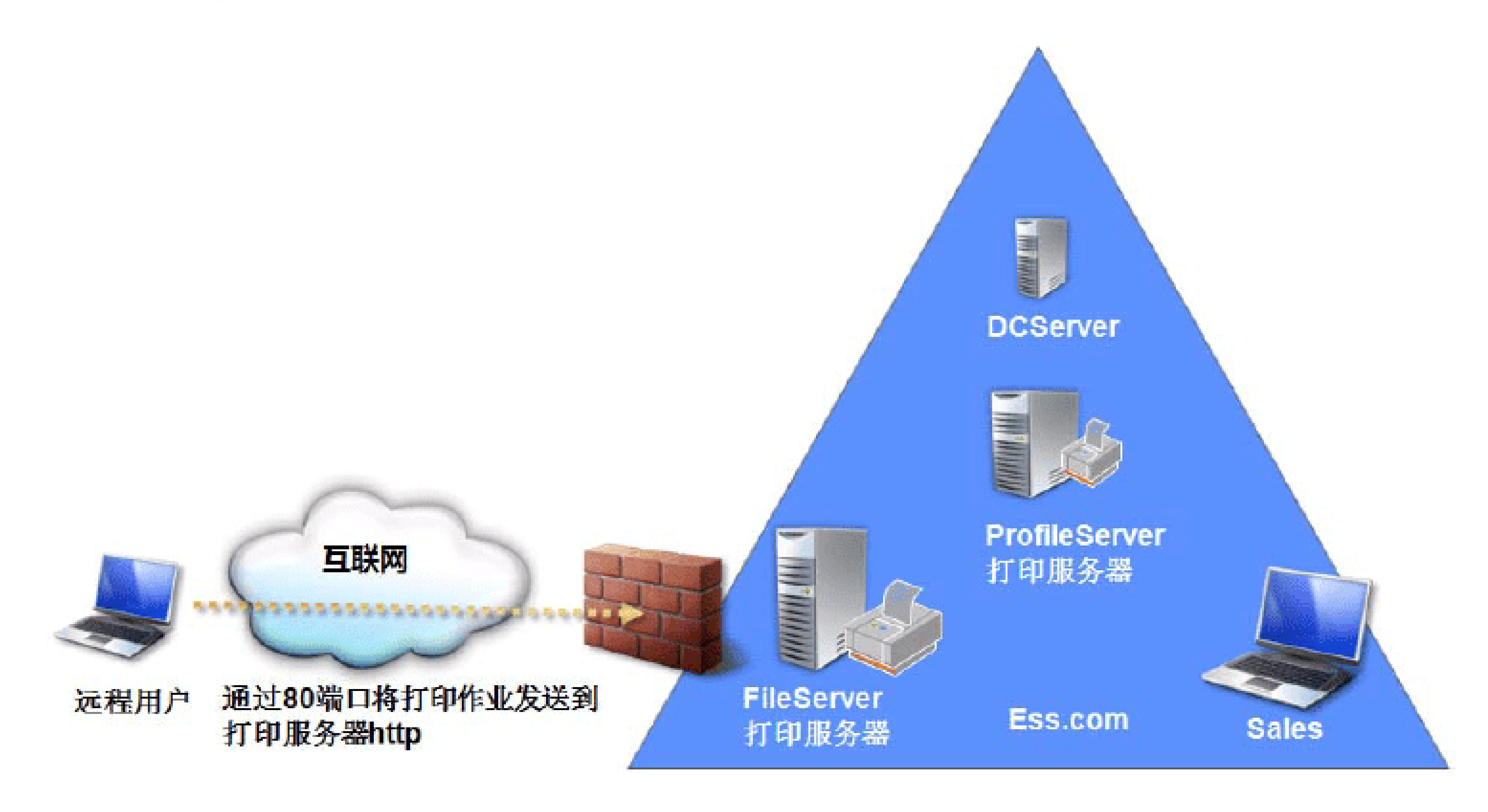


图 10-1 实战环境

- DCServer 安装了 Windows Server 2008 企业版操作系统。
- FileServer 安装了 Windows Server 2008 企业版操作系统，能够通过互联网访问到该服务器。
- ProfileServer 安装了 Windows Server 2008 企业版核心。
- Sales 安装了 Vista 操作系统。

实战目标

- 学会在打印服务器添加本地打印机并共享打印机。
- 设置打印服务器属性。
- 授权打印服务器使用。
- 设置打印池。
- 设置打印优先级。
- 将打印机发布到活动目录。
- 配置 Http 打印。

10.2.1 任务 1：配置打印服务器

在打印服务器上添加本地打印机(Local Printer)。

本地打印机实现本地打印，共享本地打印机后网络中的计算机可以将打印作业发送过来。本地打印机通过使用 LPT、USB 或 IR 接口来连接打印设备，如图 10-2 所示。

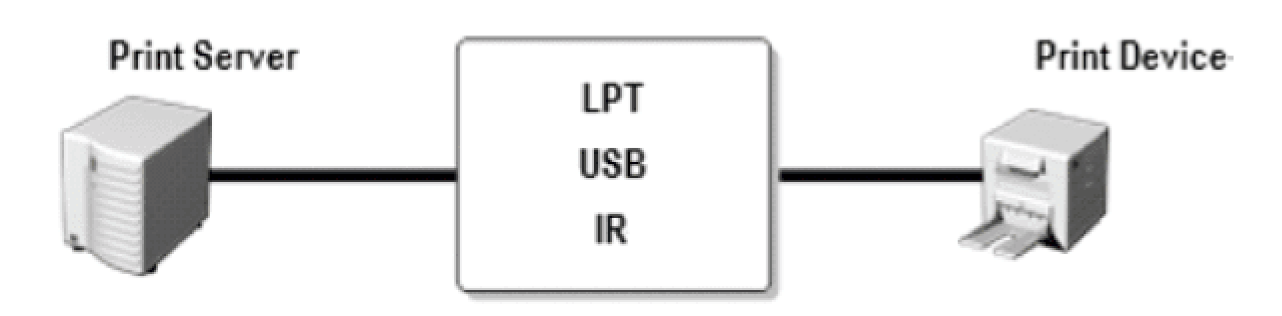


图 10-2 本地打印机接口

本地打印机也可以通过使用 IP 或 IPX 协议来连接到网络打印设备，这样的打印机称为网络接口打印机，并且支持即插即用。

① 以域管理员账户登录 FileServer，如图 10-3 所示，打开服务器管理器，单击“添加角色”按钮，打开“添加角色向导”对话框。

② 如图 10-4 所示，在“选择服务器角色”界面中，选中“打印服务”复选框，单击“下一步”按钮。



提示：使用 Windows Vista 和 Windows Server 2008 中的打印服务，可以在网络上共享打印机，而且可以使用“打印管理”Microsoft 管理控制台 (MMC) 管理单元集中执行打印服务器和网络打印机的管理任务。“打印管理”可以帮助用户监视打印队列，并在打印队列停止处理打印作业时接收通知。此外，使用该服务，还可以使用组策略迁移打印服务器并部署打印机连接。

③ 如图 10-5 所示，在“选择角色服务”界面中，选中“打印服务器”、“LPD 服务”和“Internet 打印”复选框。在出现的对话框中，单击“添加必要的角色服务”按钮，单击“下一步”按钮。如图 10-6 所示，在“Web 服务器(IIS)”界面中，单击“下一步”按钮。

④ 如图 10-7 所示，在“选择角色服务”界面中，保持默认设置。单击“下一步”按钮。

⑤ 如图 10-8 所示，在“确认安装选择”界面中，单击“安装”按钮。

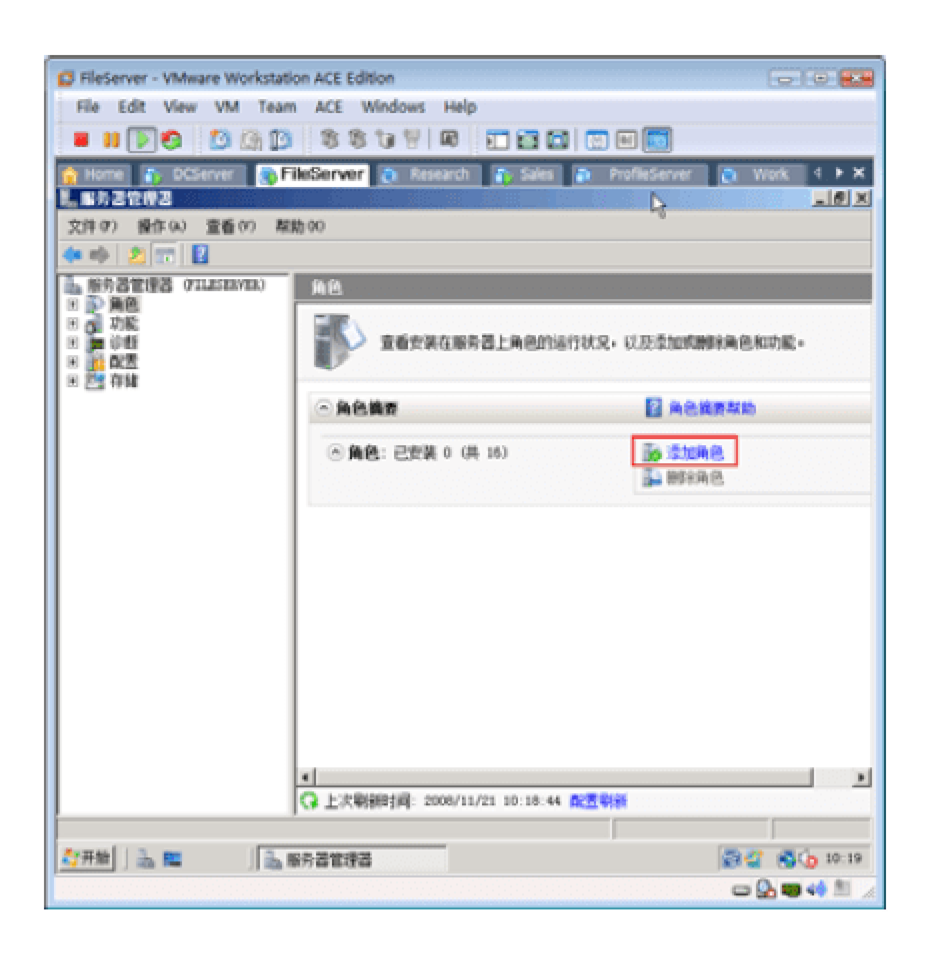


图 10-3　添加角色

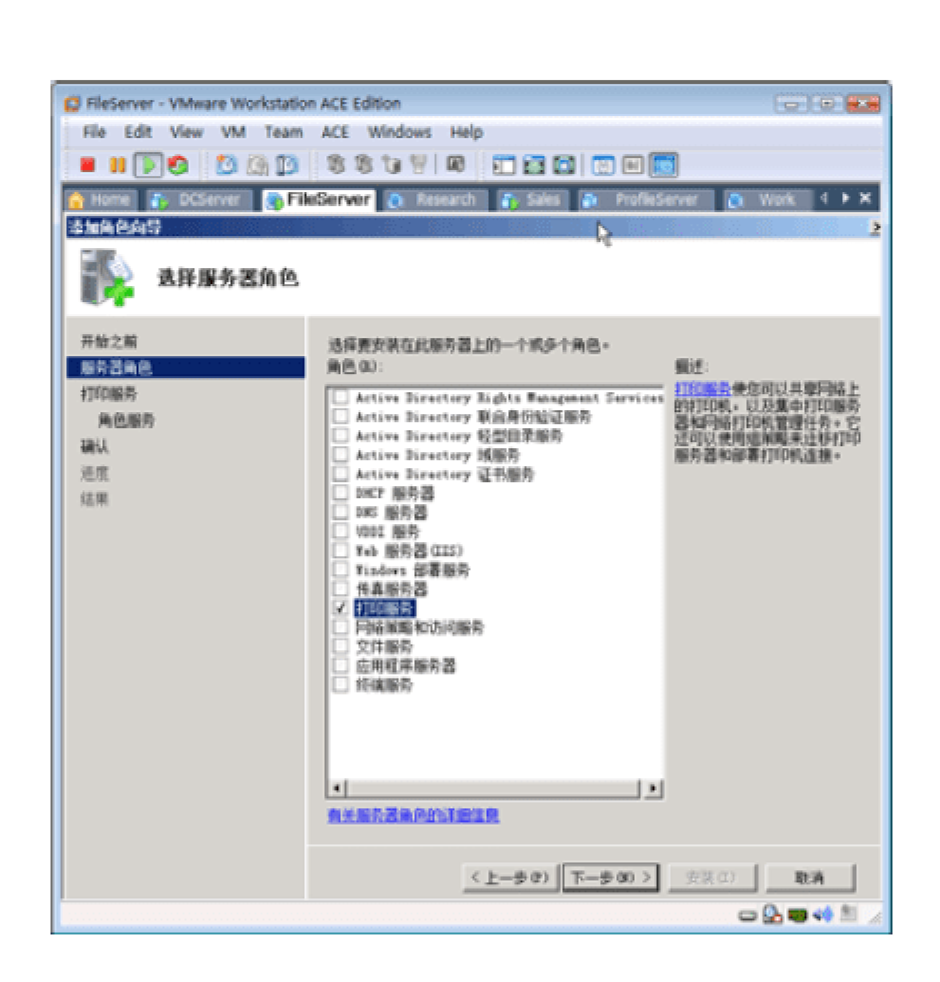


图 10-4　选择角色

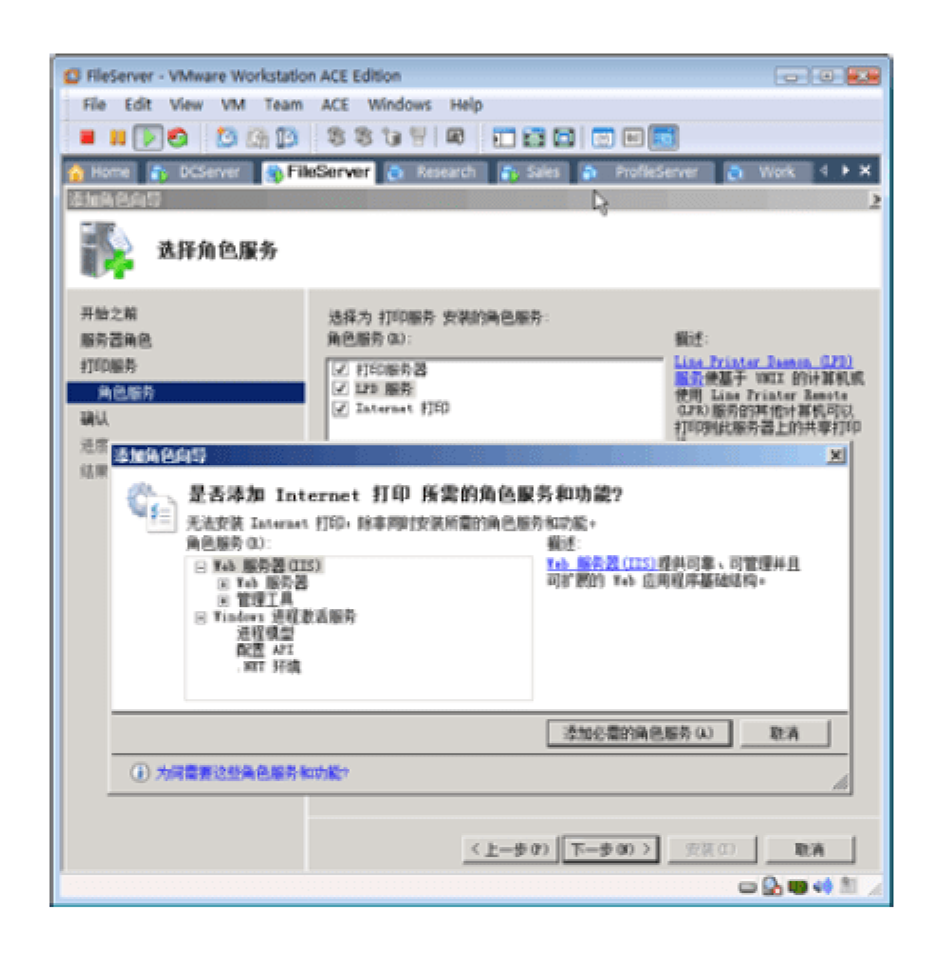


图 10-5　添加必要的角色

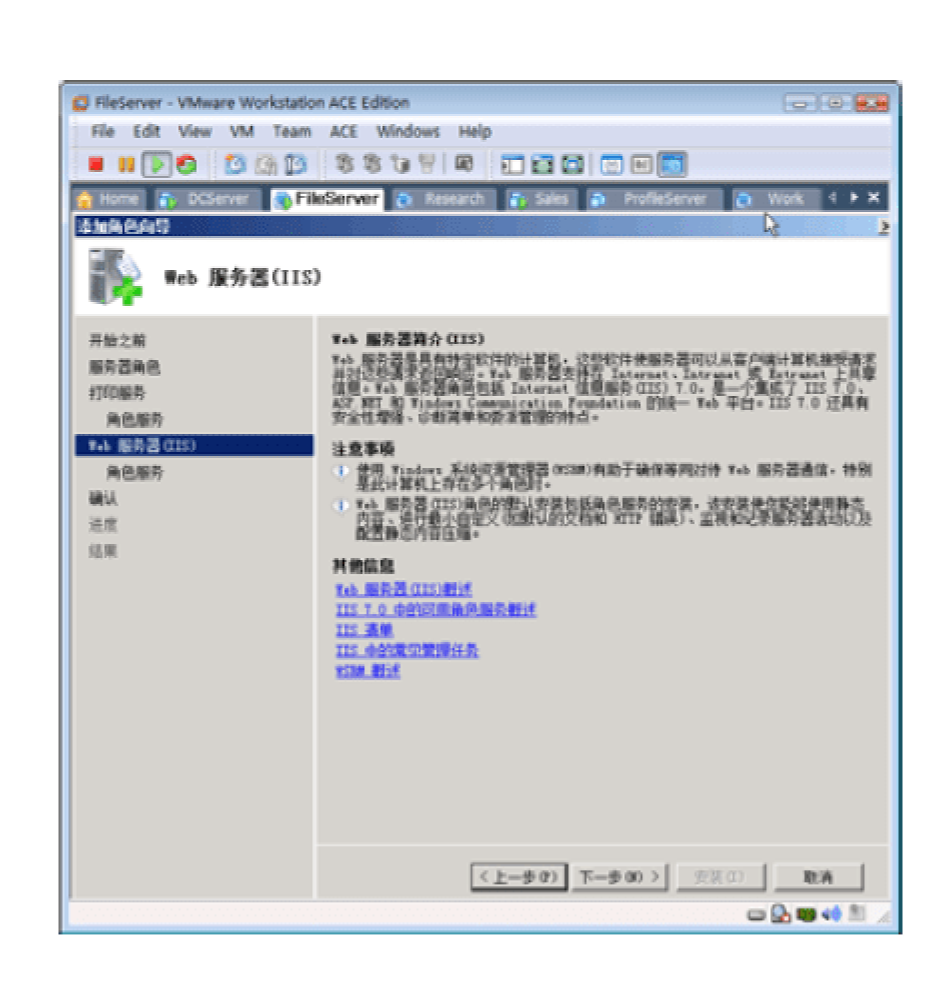


图 10-6　安装 IIS 角色

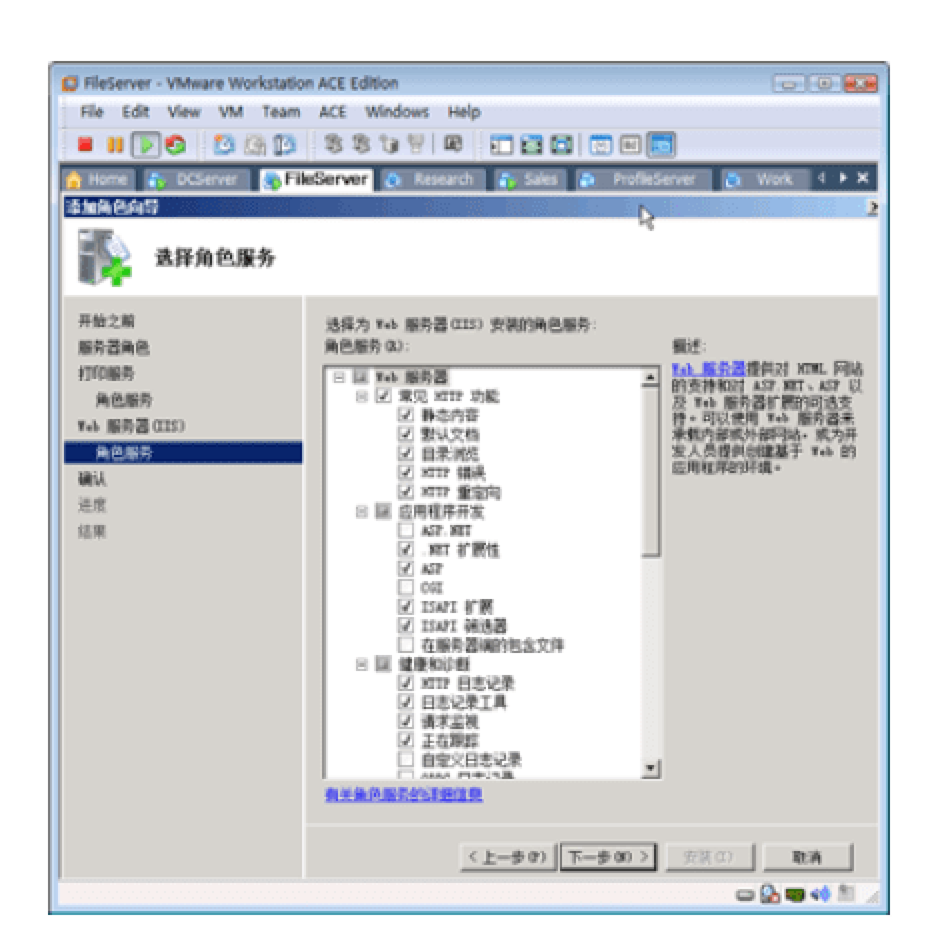


图 10-7　选择角色服务

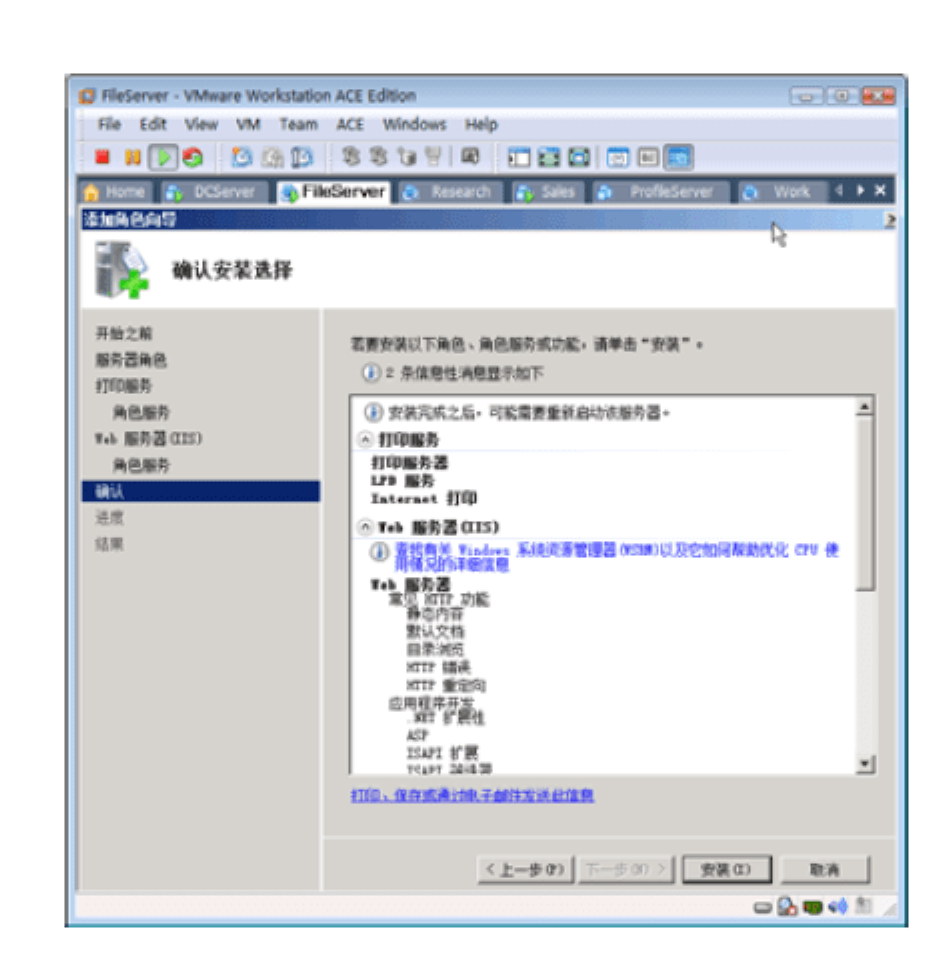


图 10-8　确认安装

⑥ 安装完成后，选择“开始”→“程序”→“管理工具”→“打印管理”命令。

⑦ 如图 10-9 所示，在“打印管理”窗口中右击 FileServer(本机)，从弹出的快捷菜单中选择“添加打印机”命令，将打开“网络打印机安装向导”对话框。

⑧ 如图 10-10 所示，在“打印机安装”界面中选中“使用现有的端口添加新打印机”单选按钮，选中连接打印机的端口。

注意：选择在网络中搜索打印机，实质上是连接一个其他服务器已经共享了的打印机。选择按 IP 地址或主机名添加 TCP/IP 或 Web 服务打印，就是连接网络接口打印机。

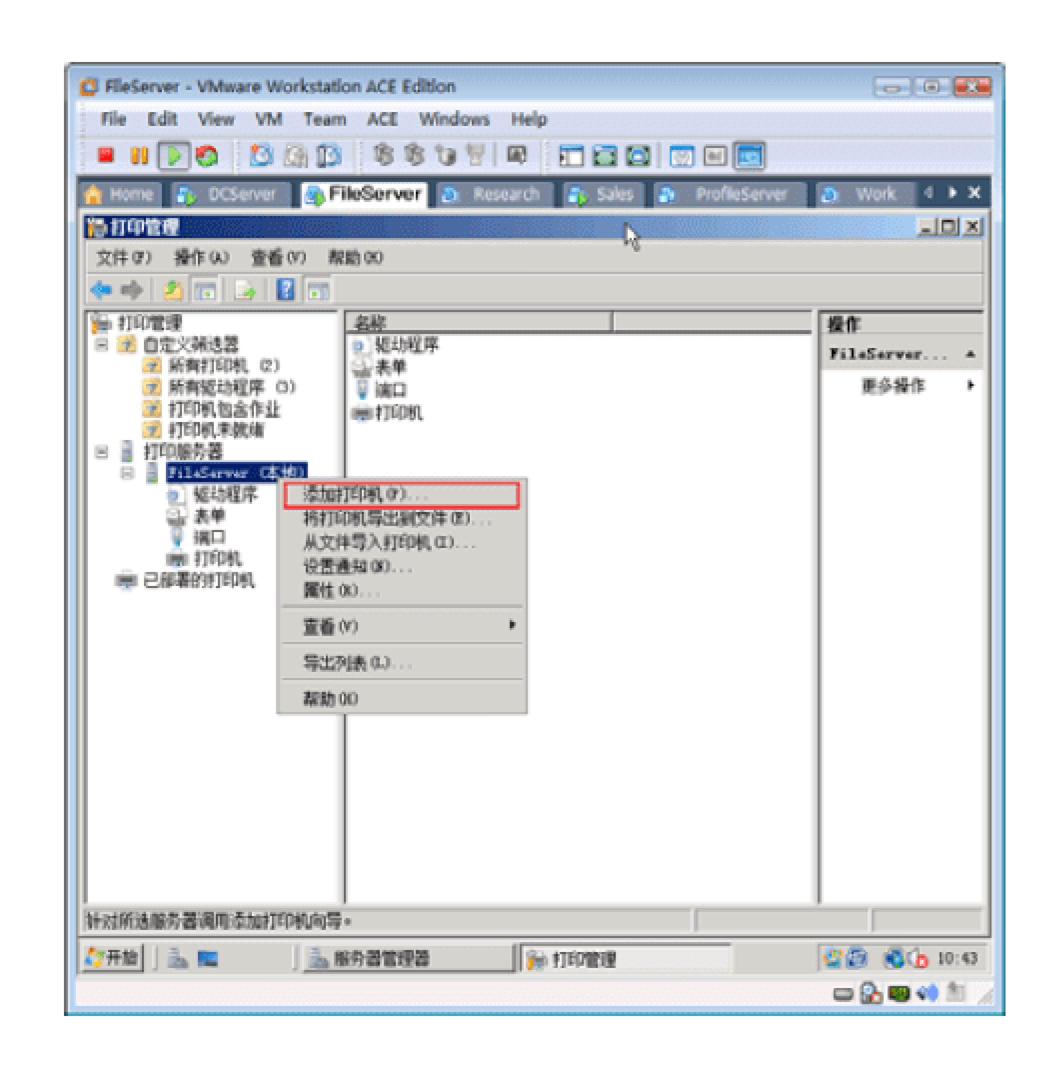


图 10-9　添加打印机

图 10-10　选择端口

⑨ 如图 10-11 所示，在“打印机驱动程序”界面中，选中“安装新驱动程序”单选按钮，单击“下一步”按钮。

⑩ 如图 10-12 所示，在“打印机安装”界面中，选择一个厂商并选中一种打印机型号，单击“下一步”按钮。

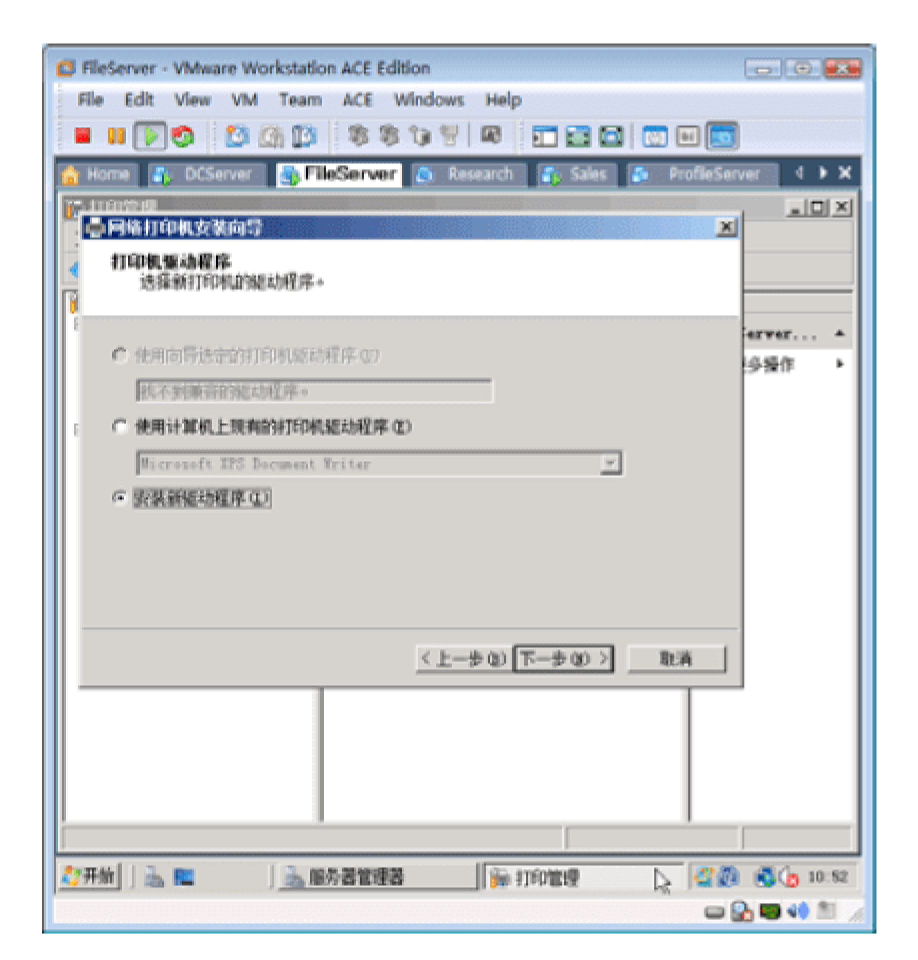


图 10-11　安装新驱动

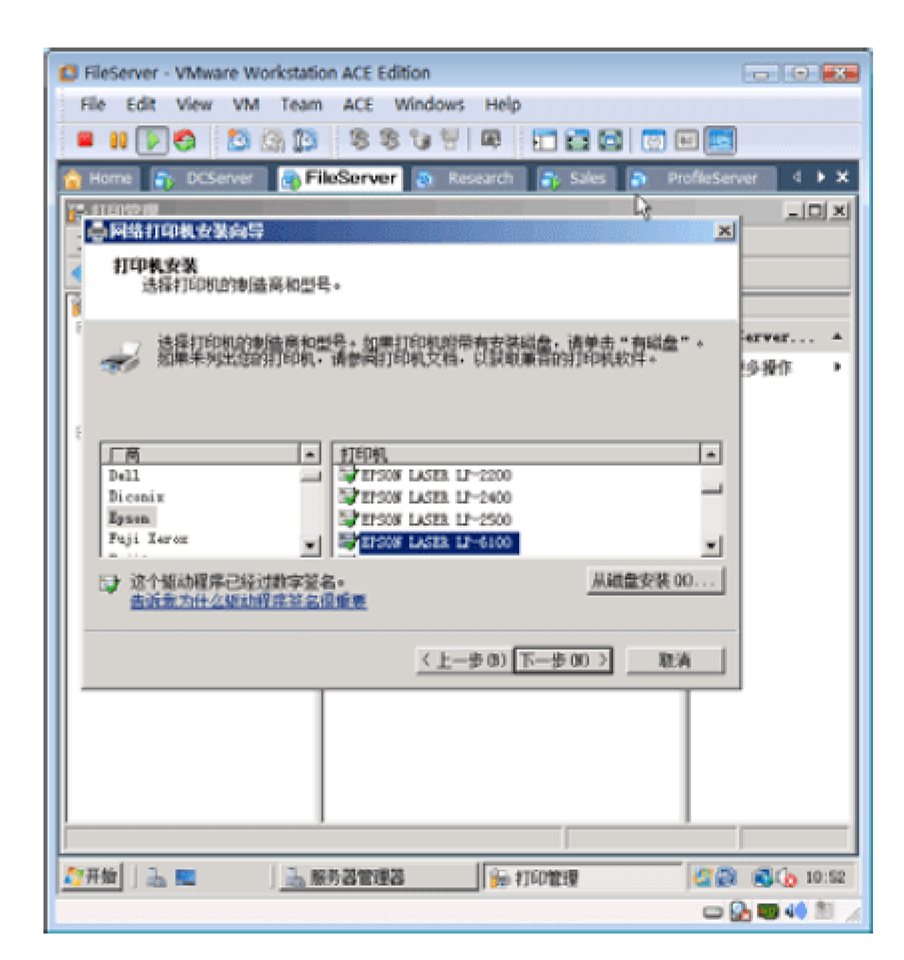


图 10-12　选择厂商和打印机类型

注意：凡是能够列出来的厂商的打印机设备驱动，都支持即插即用，只要将打印设备接好，驱动会自动安装，不需要这样添加；如果没有接硬件而添加驱动，只能这样添加。

⑪　如图 10-13 所示，在“打印机名称和共享设置”界面中，输入打印机名以及共享名称，单击“下一步”按钮。

⑫　如图 10-14 所示，在“找到打印机”界面中，单击“下一步”按钮，完成驱动安装。

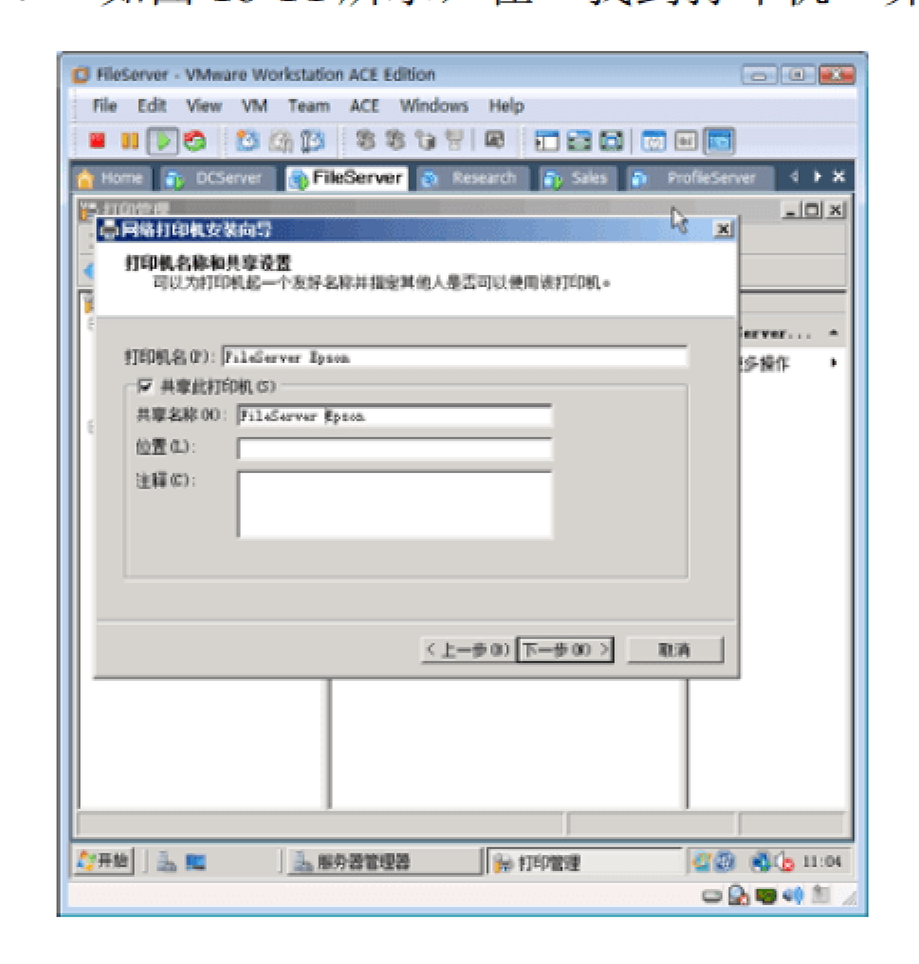


图 10-13　共享打印机

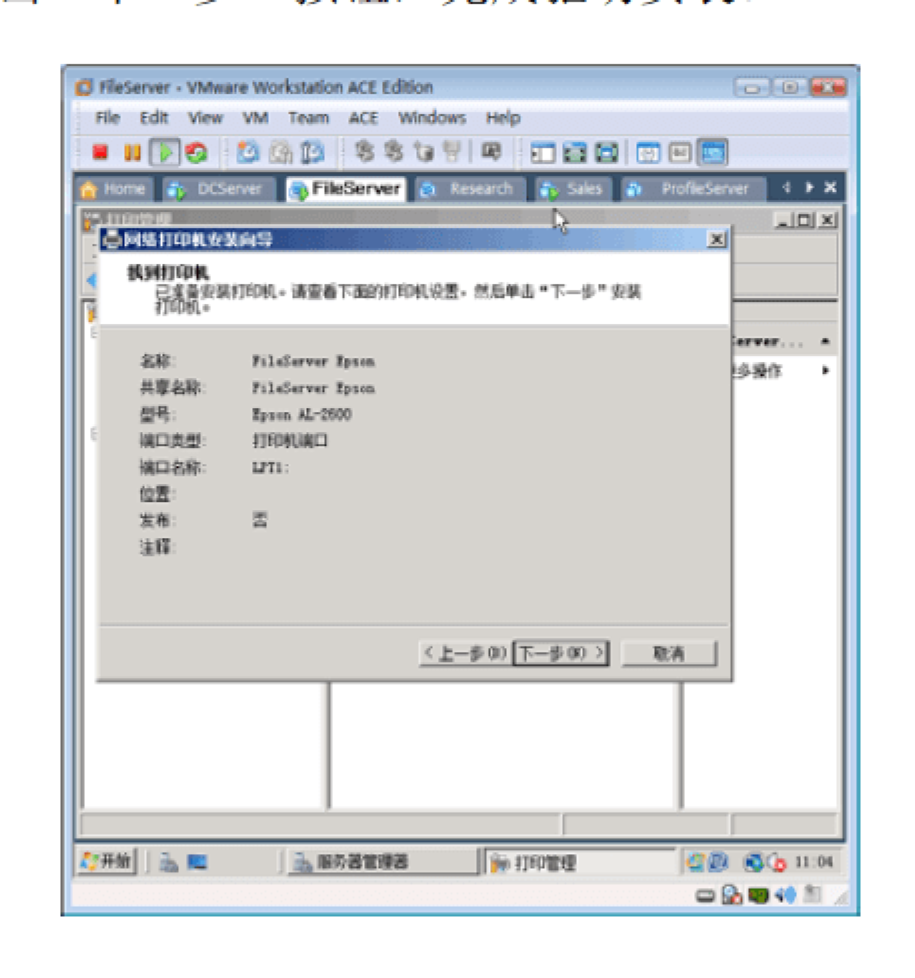


图 10-14　完成安装打印机

10.2.2　任务 2：设置后台打印文件夹的位置

如果用户向打印服务器发送太多的打印作业，打印服务默认存储打印作业的磁盘空间也许不够用，这时可以更改设置后台打印文件夹的位置。

如图 10-15 所示，右击打印服务器，在弹出的快捷菜单中选择“属性”命令，在出现的“打印服务器 属性”对话框的“高级”选项卡中，可以更改后台打印文件夹位置。

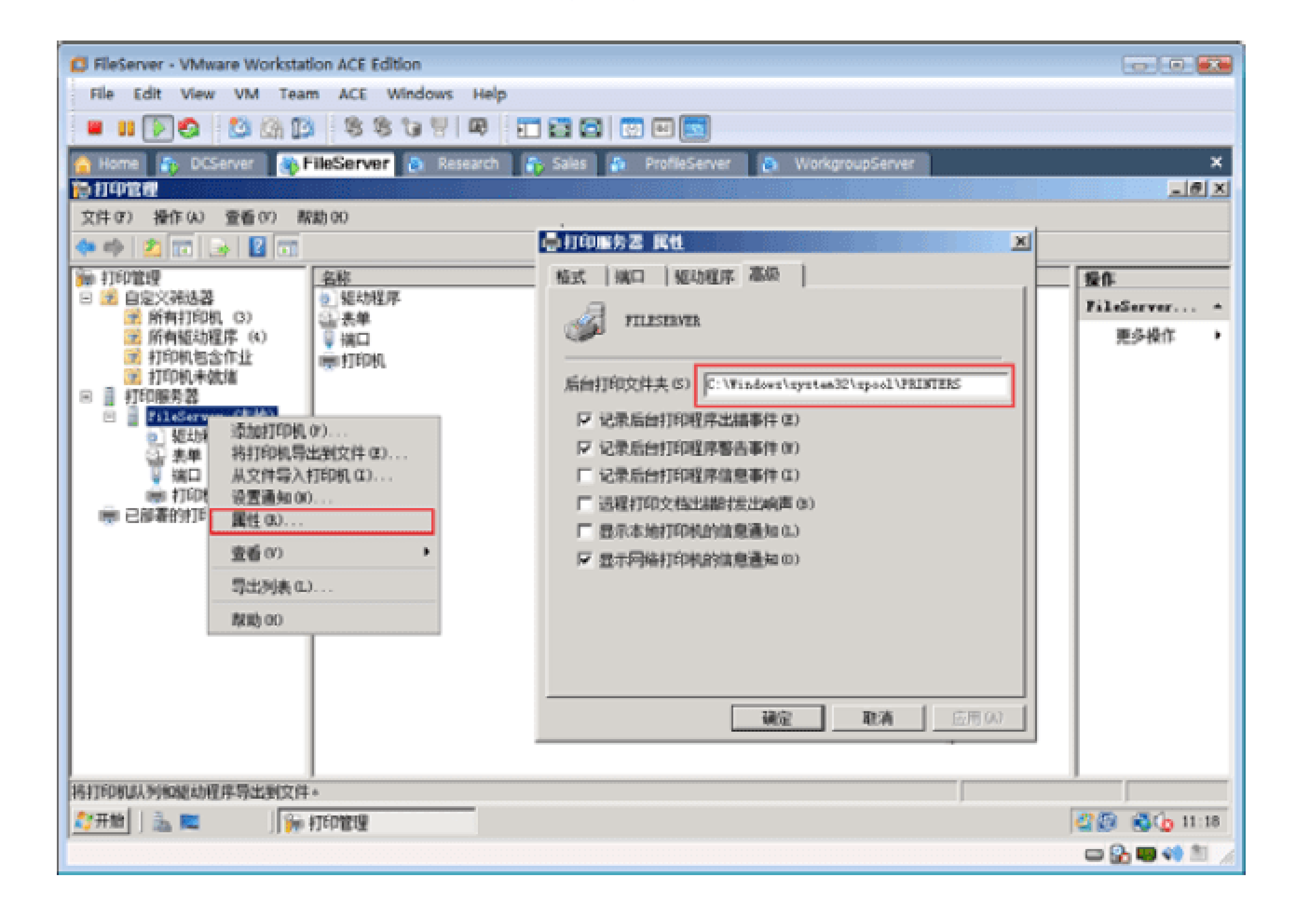


图 10-15　配置后台打印文件存放位置

10.2.3 任务 3：使用网络打印机

在 Sales 计算机上连接打印服务器 FileServer 计算机上的共享打印机。

① 以域管理员账号登录到 Sales，选择“开始”→“设置”→“打印机”命令，可以看到在 Sales 计算机上可用的打印机。

② 选择“开始”→“运行”命令，在打开的“运行”对话框中输入“\\FileServer”，如图 10-16 所示。单击“确定”按钮。

③ 如图 10-17 所示，可以看到 FileServer 计算机上共享的打印机。右击共享的打印机，从弹出的快捷菜单中选择“连接”命令。

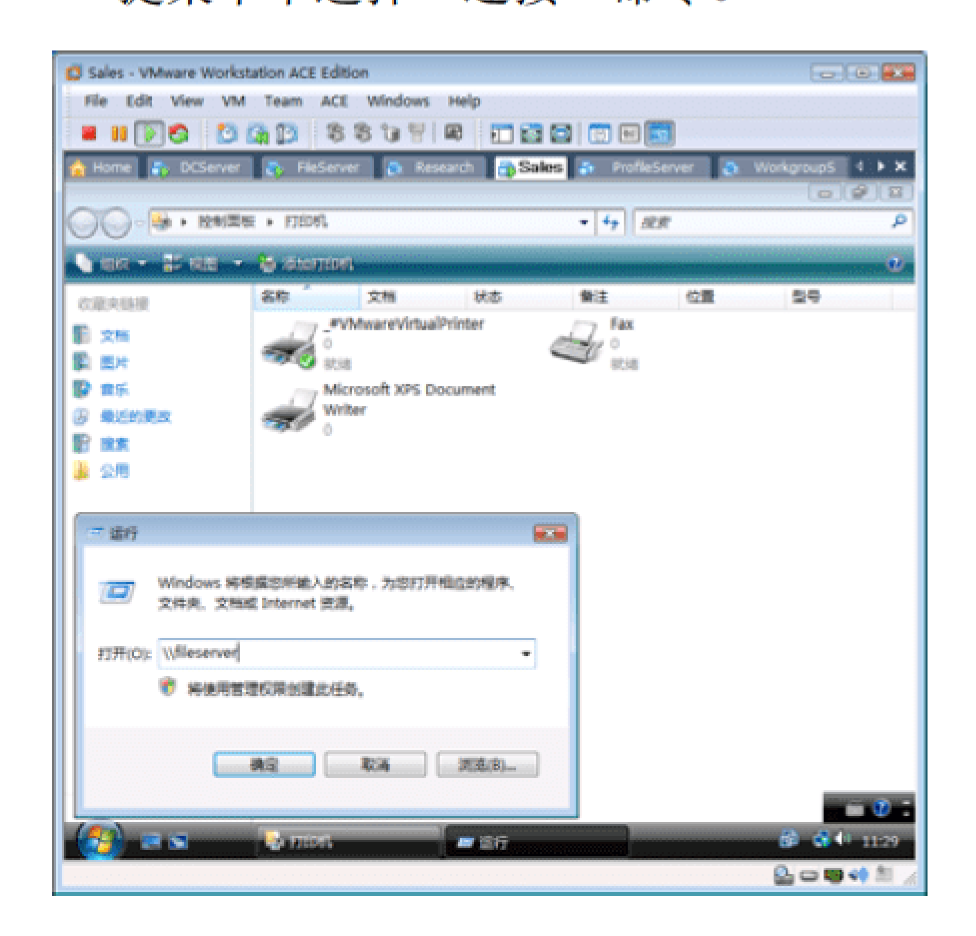


图 10-16　访问共享的打印机

图 10-17　添加网络打印机

④ 如图 10-18 所示，可以看到连接的网络打印机。

⑤ 如图 10-19 所示，创建一个记事本文件，选择“文件”→“打印”命令，在出现的“打印”对话框中选中连接的 FileServer 上的打印机，单击“打印”按钮。

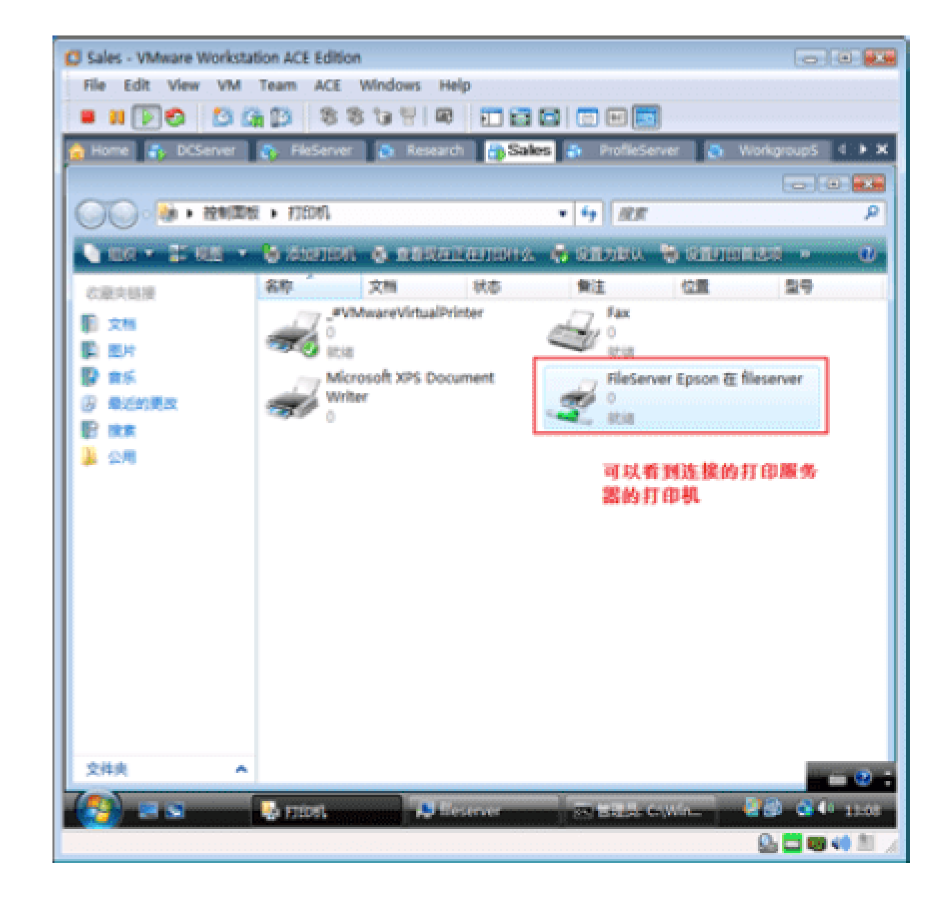


图 10-18　连接的网络打印机

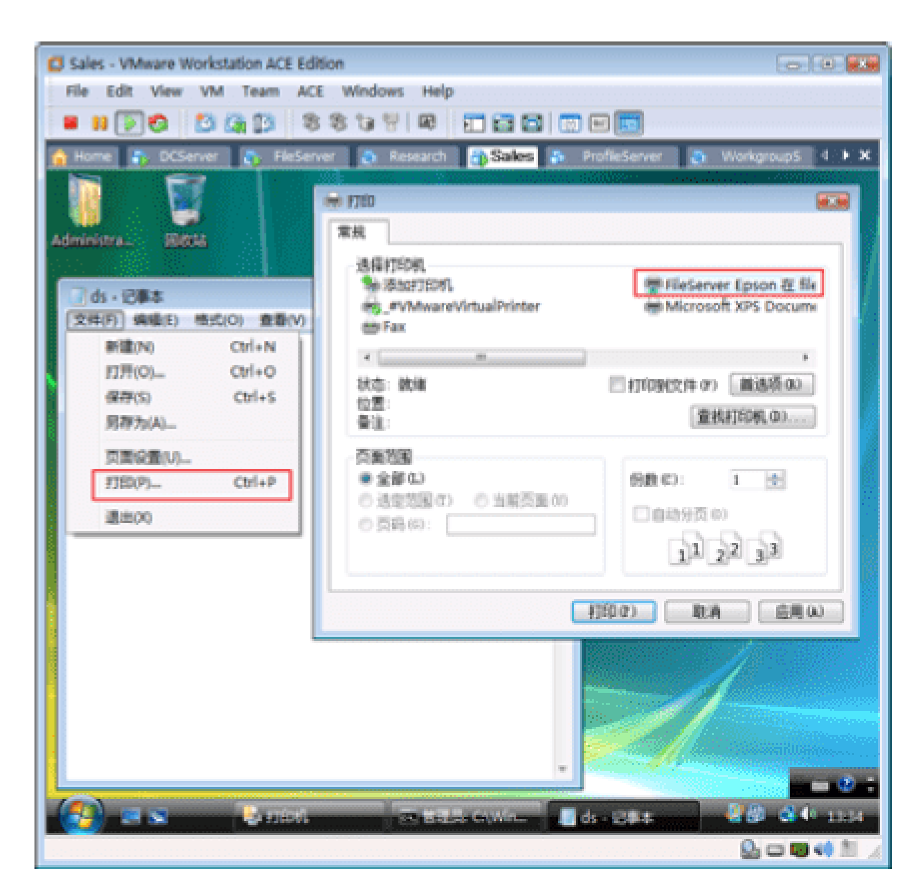


图 10-19　使用网络打印机打印

⑥ 如图 10-20 所示，单击工具栏中的按钮，可以看到打印作业。可以停止、暂停或取消打印作业。

⑦ 如图 10-21 所示，在文件服务器上，选择“开始”→“设置”→“打印机”命令。双击 FileServer Epson 可以看到所有发过来的打印作业。

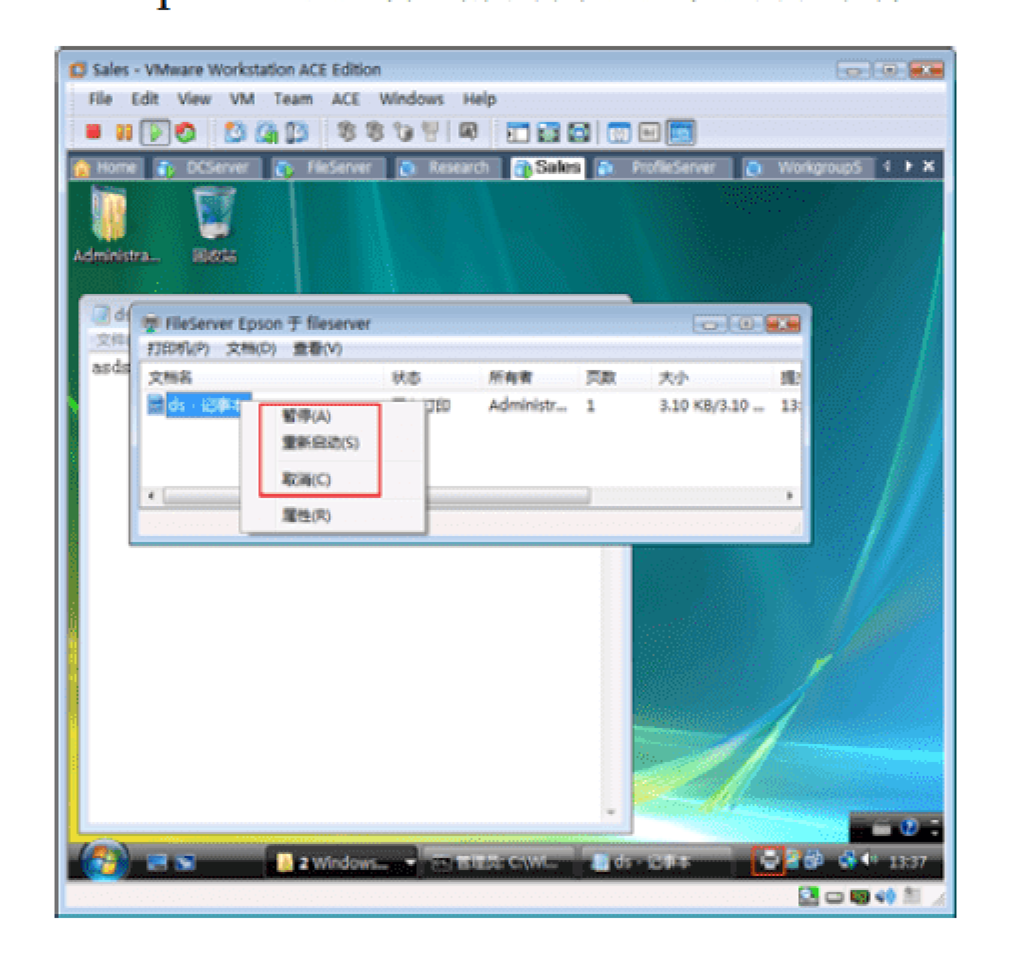


图 10-20　管理打印作业

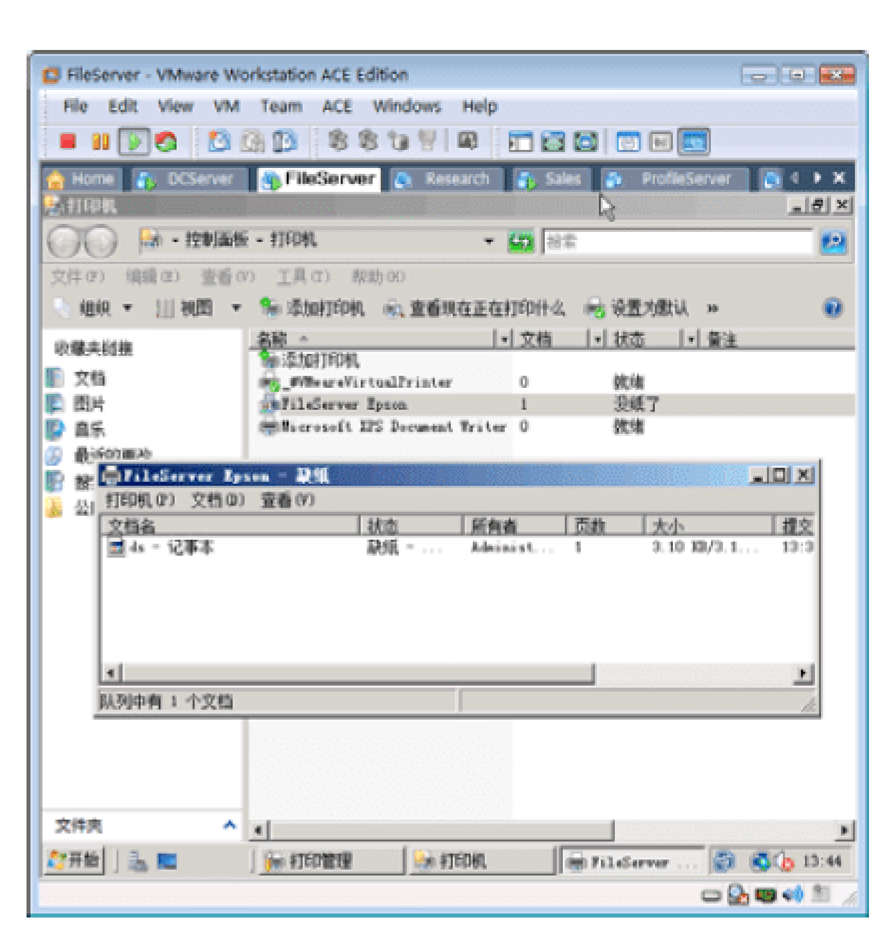


图 10-21　在打印服务器上管理打印作业

10.3　设置打印权限

10.3.1　打印机权限概述

将打印机安装在网络上后，系统会为它指派默认的打印机权限，该权限允许所有用户访问打印机并进行打印，也允许管理员选择组来对打印机和发送给它的打印文档进行管理。由于打印机可用于网络上的所有用户，因此可能需要管理员通过指派特定的打印机权限，来限制某些用户的访问权。例如，可以给部门中所有无管理权的用户设置 Print 权限，而给所有管理人员设置 Print 和 Manage Document 权限。这样，所有用户和管理人员都能打印文档；但管理人员还能更改发送给打印机的任何文档的打印状态。

Windows 提供了以下三种等级的打印安全权限。

■ 打印(Print)

使用打印权限，用户可以连接到打印机，并将文档发送到打印机。在默认情况下，打印权限将指派给 Everyone 组中的所有成员。

■ 管理打印机(Manage Printers)

使用管理打印机权限，用户可以执行与打印权限相关联的任务，并且具有对打印机的完全管理控制权。用户可以暂停和重新启动打印机、更改打印后台处理程序设置、共享打印机、调整打印机权限，还可以更改打印机属性。默认情况下，管理打印机权限将指派给 Administrators 组和 Power Users 组的成员。

■ 管理文档(Manage Documents)

使用管理文档权限，用户可以暂停、继续、重新开始和取消由其他所有用户提交的文档，还可以重新安排这些文档的顺序。但是，用户无法将文档发送到打印机或控制打印机状态。默认情况下，管理文档权限指派给 Creator Owner 组的成员。

当用户被指派管理文档权限时，用户将无法访问当前等待打印的现有文档。此权限只应用于在该权限被指派给用户之后发送到打印机的文档。


注意：默认情况下，Administrators 组和 Power Users 组的成员拥有完全访问权限，即这些用户拥有打印、管理文档以及管理打印机的权限。

当给一组用户指派了多个权限时，将应用限制性最少的权限。但是，当应用了拒绝(Deny)权限时，它将优先于其他任何权限。 如果用户对打印机的访问被拒绝，用户将无法使用或管理打印机，或者更改任何权限。

Windows 将打印机权限指派给六组用户，这些组包括：

- 管理员(Administrators)。
- 创建者所有者(Creator Owner)。
- 每个人(Everyone)。
- 特权用户(Power Users)。
- 打印操作员(Print Operators)。
- 服务器操作员(Server Operators)。

默认情况下，每组都会被指派打印、管理文档和管理打印机权限的一种组合，如表 10-1 所示(表中用×表示某组具有相应的权限)。

表 10-1 用户组权限

组	打 印	管理文档	管理打印机
Administrators	×	×	×
Creator Owner		×	
Everyone	×		
Power Users	×	×	×
Print Operators	×	×	×
Server Operators	×	×	×


注意：Print Operators 和 Server Operators 组仅存在于域控制器。

每个权限都由一组允许用户执行特定任务的特殊权限组成。表 10-2 总结了与每种打印安全权限关联的访问级别(表中用×表示与某任务关联的访问级别)。

表 10-2 打印安全权限关联的访问级别

允许的任务	打 印	管理文档(只适用于文档)	管理打印机
打印	×		×
管理打印机			×
管理文档		×	
读取权限	×	×	×
更改权限		×	×
取得所有权		×	×

10.3.2　管理访问打印机

当一个共享打印机被安装到网络上时，默认的打印机权限将允许所有的用户可以访问该打印机并进行打印。为了保证安全性，管理员可以选择指定的用户组来管理发送到打印机的文档，可以选择指定的用户组来管理打印机，也可以明确地拒绝指定的用户或组对打印机的访问。

管理员可能想通过授予明确的打印机权限来限制一些用户对打印机的访问。例如，管理员可以给部门中所有无管理权的用户设置 Print 权限，而给所有管理人员设置 Print 和 Manage Document 权限。这样，所有用户和管理人员都能打印文档，但只有管理人员才能更改发送给打印机的任何文档的打印状态。

有些情况下，管理员可能想给某个用户组授予访问打印机的权限，但同时又想限制该组中的若干成员对打印机的访问。在这种情况下，管理员可以先为整个用户组授予可以访问打印机的权限(Allow 权限)，然后再为该组中指定的用户授予拒绝(Deny)权限。

管理员可以通过以下步骤来为管理打印机访问设置权限。

如图 10-22 所示，右击打印机，在弹出的快捷菜单中选择“属性”命令。在打印机属性对话框的“安全”选项卡中，单击“添加”按钮可以给用户授权或解除授权。



注意：要查看或更改构成打印操作、管理打印机和管理文档的基本权限，单击“高级”按钮。

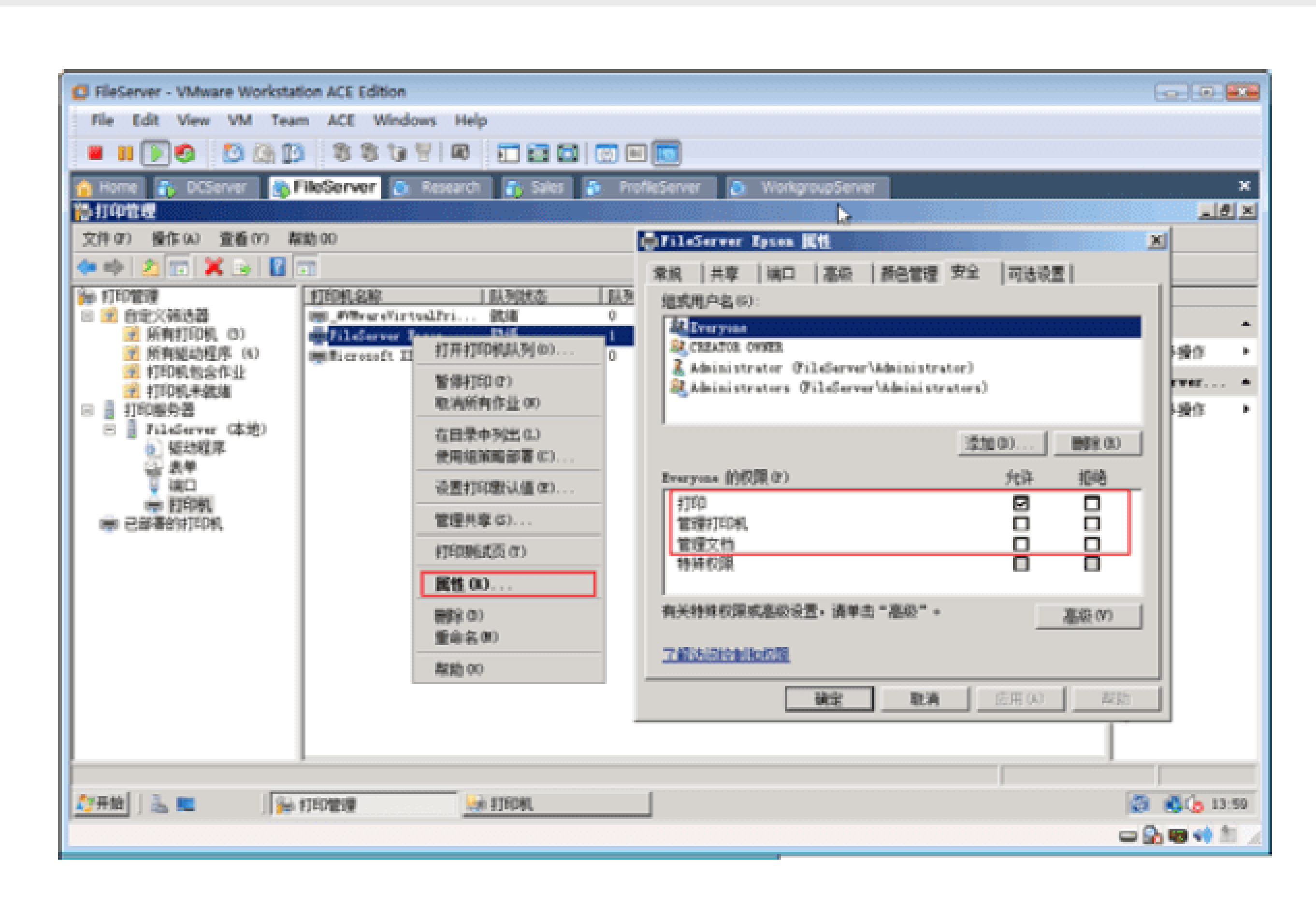


图 10-22　设置打印权限

10.4　管理打印机

10.4.1　设置打印机优先权

一个部门的普通员工经常打印一些文档，但不着急用，而领导经常打印一些短小但是急着用的文件。如果普通员工已经向打印机发送了打印任务，如何让领导的文件优先打印呢？

在打印机之间设置优先权可以优化到同一台打印设备的文档打印，即可以加速需要立即打印的文档。

高优先级的用户发送来的文档可以越过等候打印的低优先级的文档队列。如果两个逻辑打印机都与同一打印机相关联，则 Windows Server 2008 家族操作系统首先将优先级最高的文档发送到该打印机。打印机优先权的示意图如图 10-23 所示。

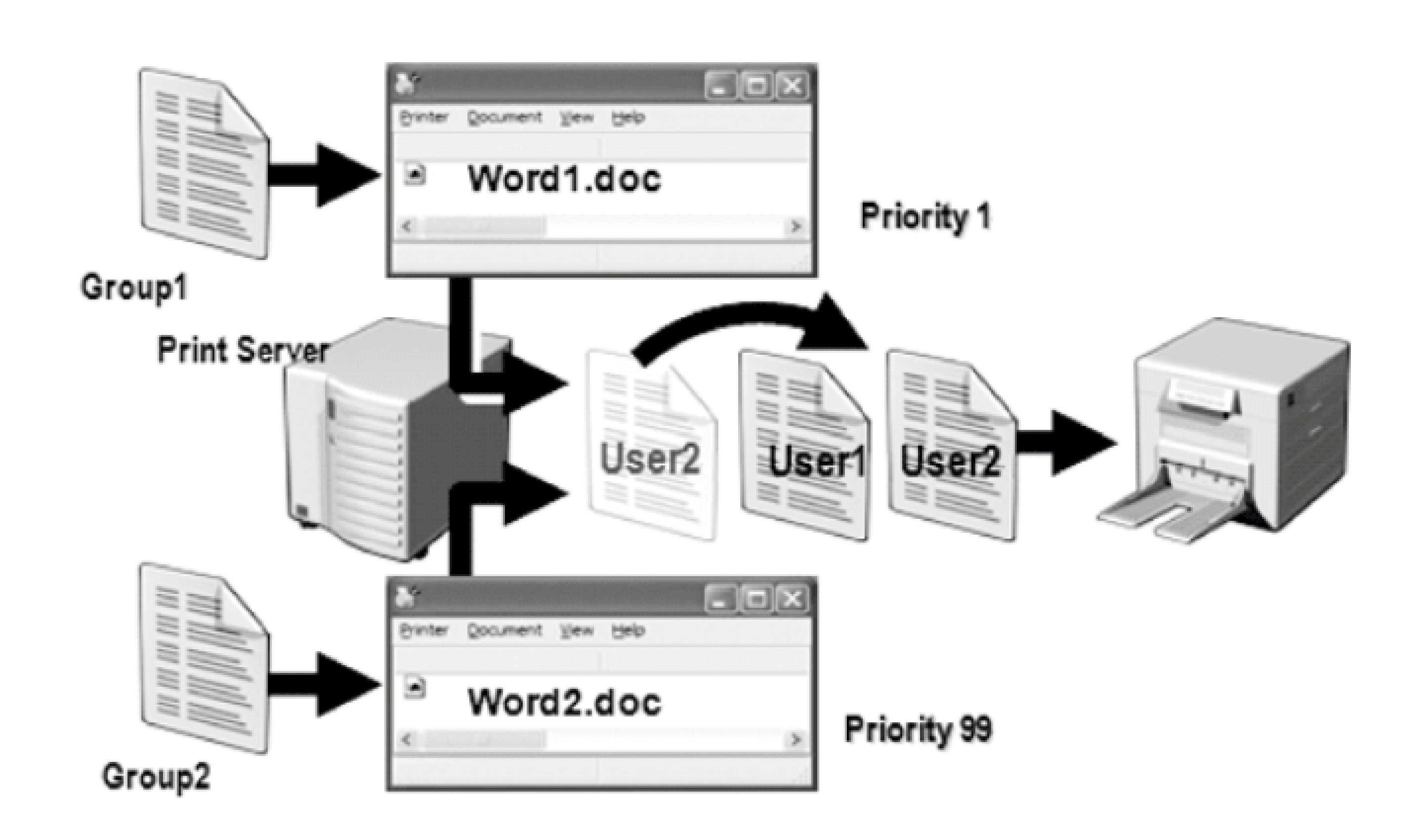


图 10-23　打印机优先权

图 10-23 中，Group1 的用户以优先级 1(最低优先级)向打印服务器发送文档 Word1.doc，Group2 的用户以优先级 99(最高优先级)向打印服务器发送文档 Word2.doc。由于 Group1 用户的优先级比 Group2 用户的优先级低，因而 Group2 用户发送的文档 Word2.doc 将被优先打印。

要利用打印优先级系统，需为同一打印机创建多个逻辑打印机。应为每个逻辑打印机指派不同的优先等级，然后创建与每个逻辑打印机相关的用户组。例如，Group1 中的用户拥有访问优先级为 1 的打印机的权利，Group2 中的用户拥有访问优先级为 2 的打印机的权利，依此类推。

领导可以将重要的文件发送到优先级高的打印机，普通员工将打印作业发送到优先级低的打印机。为了在逻辑打印机之间设置优先级，管理员必须完成以下工作。

- 将两个或多个逻辑打印机指向同一台打印设备，即相同的打印端口。这个端口既可以是打印服务器上的物理端口，也可以是指向一台打印设备网络接口的端口。
- 为连接到打印设备的每一台逻辑打印机设置优先权，然后让不同的用户组指向不同的逻辑打印机。将高优先级的文件发送到拥有高优先权的打印机，将低优先级的文件发送到拥有低优先权的打印机。
- 优先级高的打印机只授权领导有打印权，普通员工只能够使用优先级低的打印机。

可以通过以下步骤添加一个只允许 Managers 组使用的具有高优先级的打印机。

① 如图 10-24 所示，右击打印机，从弹出的快捷菜单中选择“添加打印机”命令。选择上一次添加 Epson 打印机使用的相同的端口。

② 如图 10-25 所示，在“打印机驱动程序”界面中，选中“使用计算机上现有的打印机驱动程序”单选按钮，从下拉列表中选择 Epson AL-2600，单击“下一步”按钮。

③ 如图 10-26 所示，指定打印机名和共享名称，单击“下一步”按钮，完成安装。

④ 如图 10-27 所示，右击刚才添加的打印机，在弹出的快捷菜单中选择“属性”命令。在打开的打印机属性对话框的“高级”选项卡中，将优先级设置成 99。

⑤ 如图 10-28 所示，切换到“安全”选项卡，删除 everyone 的打印权限，添加 Managers 组的打印权限。

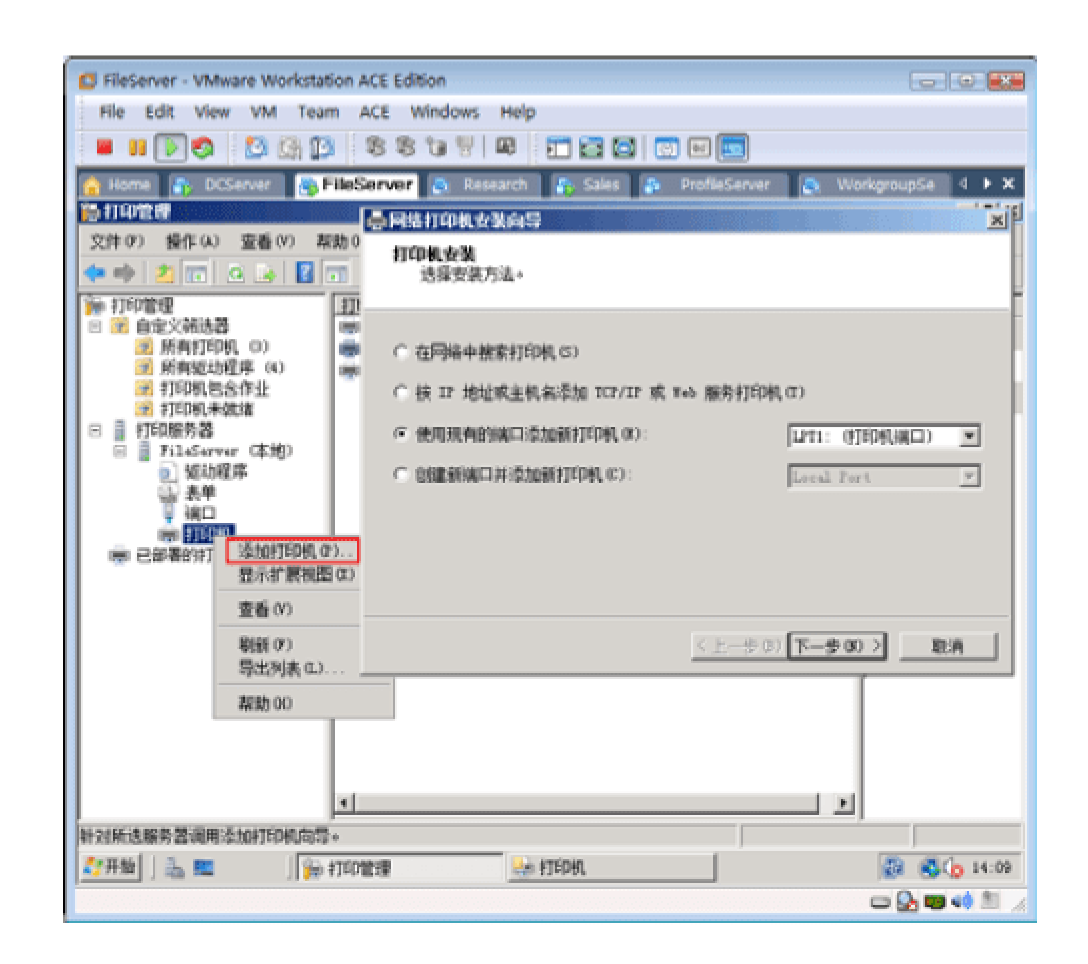


图 10-24　添加打印机

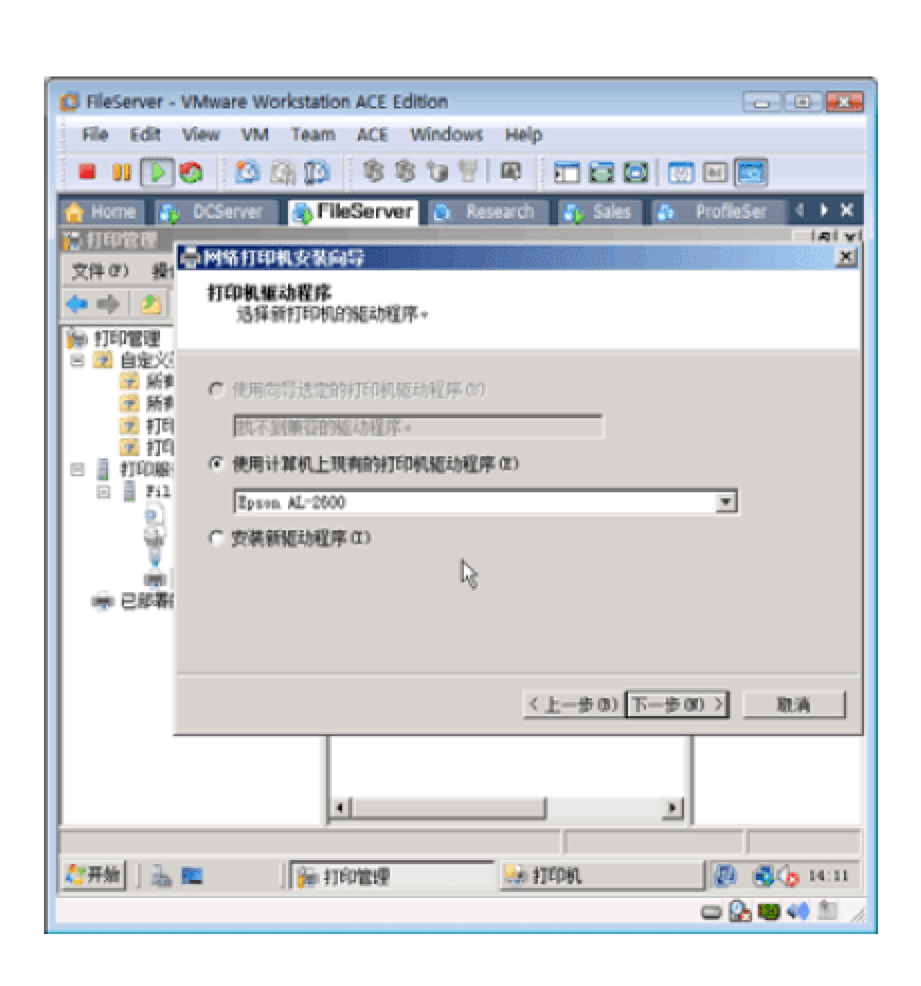


图 10-25　选择驱动程序

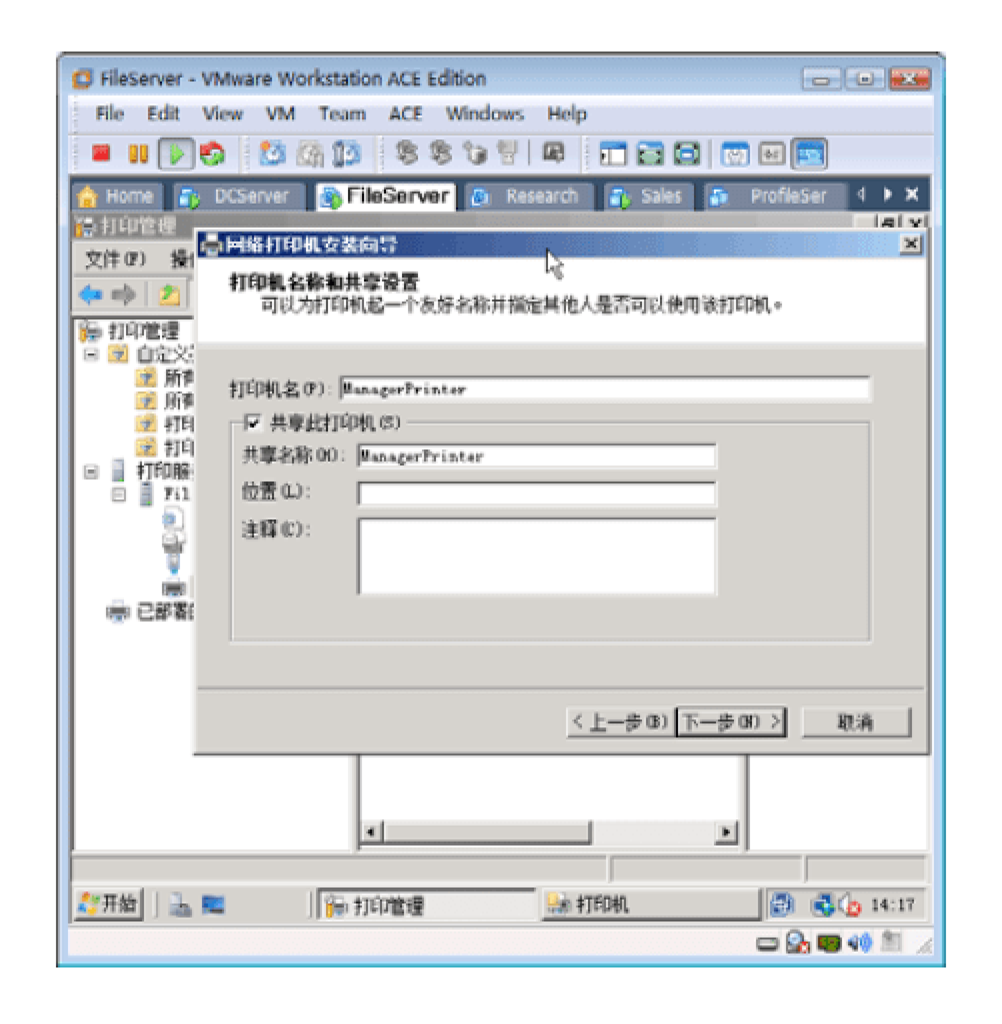


图 10-26　指定打印机名称

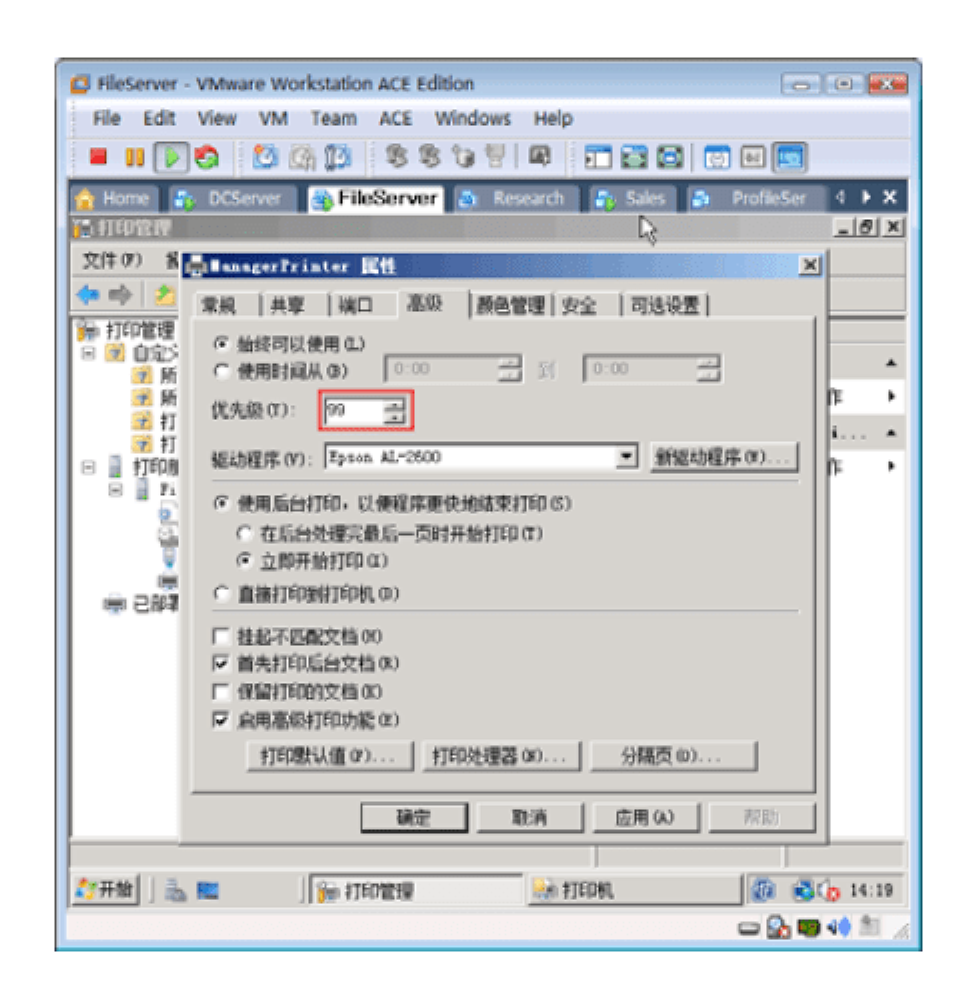


图 10-27　设置打印机优先级

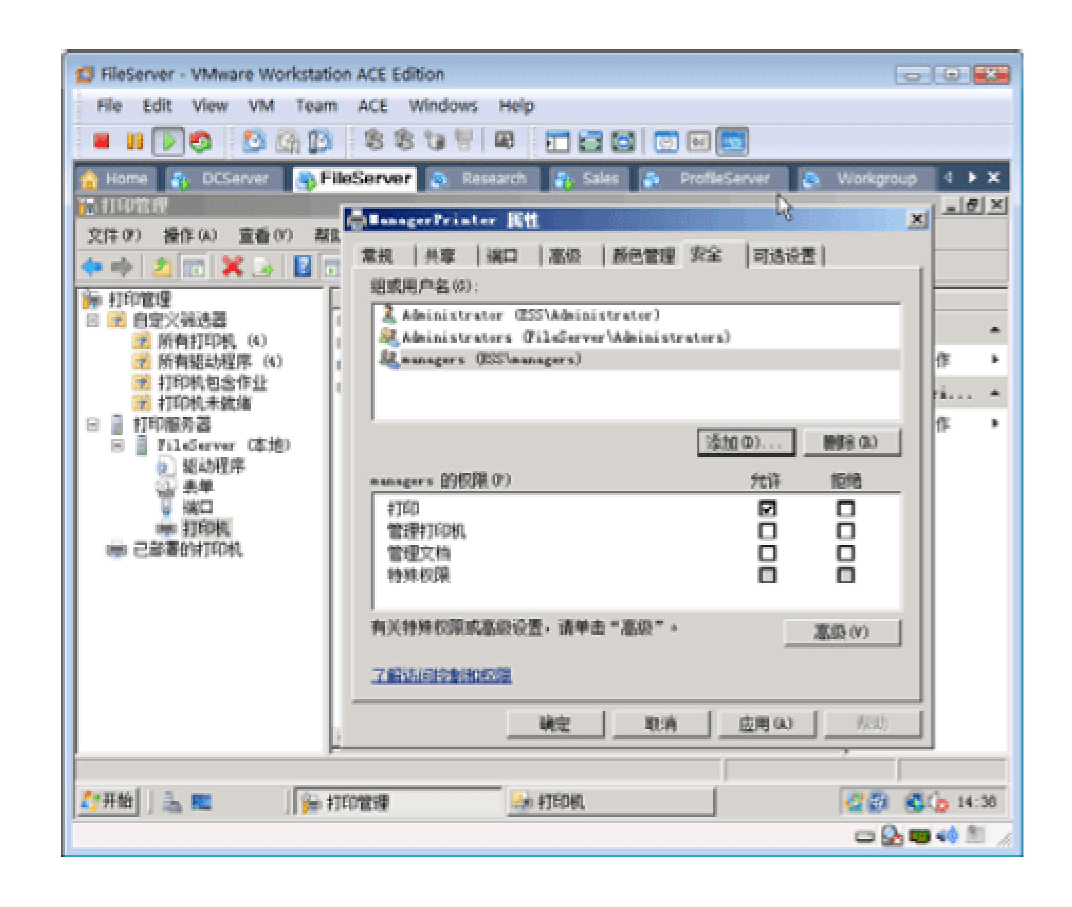


图 10-28　设置打印权限

10.4.2 计划备用打印时间

使打印机得到最大限度利用的一个有效方法是为长文档或特定类型的文档安排轮流打印时间。管理员可以在以下情况下考虑是否采用计划备用打印时间。

- **情况 1：**如果白天打印量很大，可通过将长文档路由到只在下班时间段打印的打印机，推迟这些文档的打印。打印后台处理程序持续接收文档，但是在指定的启动时间到来之前并不将这些文档发给目的地打印机。
- **情况 2：**如果不专门指定一个实际的打印设备轮流在下班时间打印(因为这样并没有使资源得到充分地利用)，可以为相同打印设备设置不同的逻辑打印机并给每一个逻辑打印机配置不同的可用时间段。例如，一台打印机可以从下午 6:00 到早上 6:00 使用，而另一个全天 24 小时可用。然后，可以通知用户将长文档发送到只有在下班时间段才可用的打印机，而将所有其他文档发送到全天可用的打印机。

管理员在计划备用打印时间时，应考虑以下建议。

- 使用安全设置来限制在可用时间段内访问打印机的用户。管理员可能想限制一个用户组只有在指定的时间段内才可以使用打印机，而允许另一个用户组可以随时使用打印机。为了实现这个目的，管理员必须创建两台指向同一台打印设备的逻辑打印机，并且管理员必须为随时使用打印机的用户组设置额外的安全性。
- 告知用户打印机什么时候可用，什么时候不可用。许多用户习惯于打印机在任何时候都是可用的，因此当他们使用有时间计划限制的打印机时，这些用户可能会尝试重新打印他们的打印作业，还有可能会打电话寻求帮助。通过告知用户打印机什么时候可用，什么时候不可用，可以帮助用户正确使用有时间计划限制的打印机。
- 配置两台指向同一打印设备的打印机，并且分别为这两台打印机设置不同的计划备用打印时间。
- 确保磁盘空间足够大，以便能够存储等待打印的后台打印作业。

计划备用打印时间

① 打开“打印管理”窗口。

② 右击想要配置的打印机，从弹出的快捷菜单中选择“属性”命令。

③ 如图 10-29 所示，在打开的打印机属性对话框中切换到“高级”选项卡。

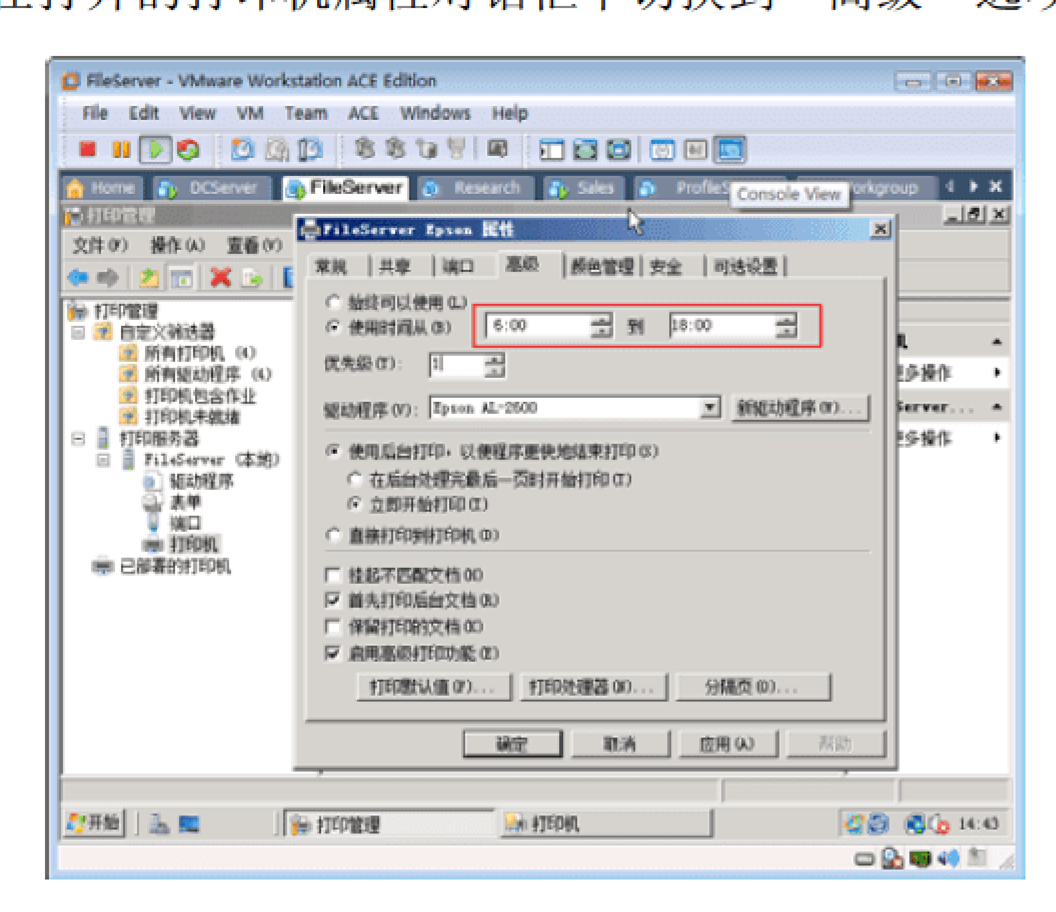


图 10-29 设置打印机时间

④　选中“使用时间从”单选按钮。

⑤　设置可以使用打印机的时间段，输入开始和终止时间，例如 6:00 到 18:00。

10.4.3　设置打印机池

用户可以通过创建打印机池(或打印池)将打印作业自动分发到下一台可用的打印机。打印池是一台逻辑打印机，它通过打印服务器的多个端口连接到多台打印机，处于空闲状态的打印机便可以接收发送到逻辑打印机的下一份文档。这对于打印量很大的网络非常有用，因为它可以减少用户等待文档打印的时间。使用打印池还可以简化管理，管理员可以从服务器上的同一台逻辑打印机来管理多台打印机。

如图 10-30 所示，在打印服务器上连接着 3 个相同的打印设备，打印服务器的打印机指向连接这三个打印设备的硬件端口。

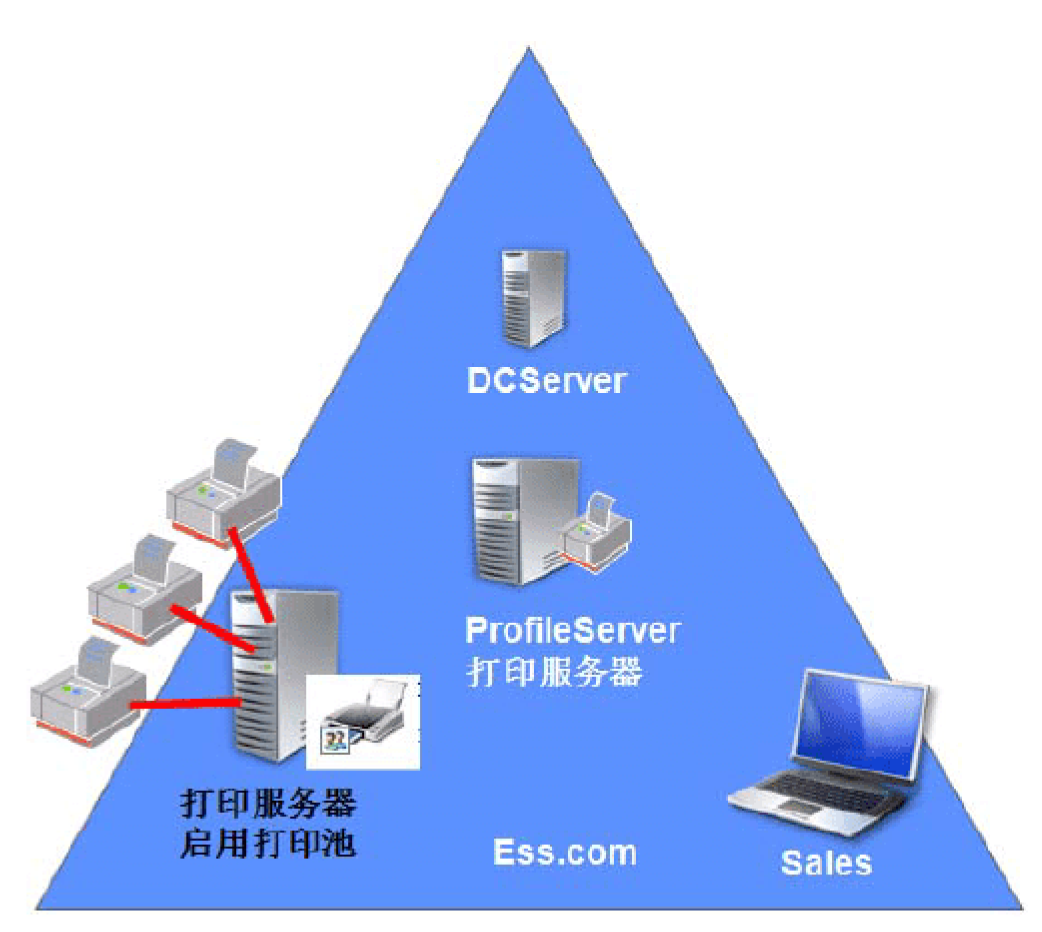


图 10-30　实战环境

使用创建的打印池，用户在打印文档时不再需要查找哪一台打印机目前可用。逻辑打印机将检查可用的端口，并按端口的添加顺序将文档发送到各个端口。应首先添加连接到快速打印机上的端口，这样可以保证发送到打印机的文档在被分配给打印池中的慢速打印机前以最快的速度打印。

用户在设置打印池之前，应考虑以下两点。

- 池中的所有打印机必须使用同样的驱动程序。
- 由于用户不知道发出的文档由池中的哪一台打印机打印，因此应将池中的所有打印机放置在同一地点。

管理员可以通过以下操作来启用打印池。

如图 10-31 所示，在“打印管理”窗口中，右击打算启用打印池的打印机，在弹出的快捷菜单中选择“属性”命令。在打开的打印机属性对话框的“端口”选项卡中，选中“启用打印机池”复选框，选择连接打印设备的端口。单击“确定”按钮。

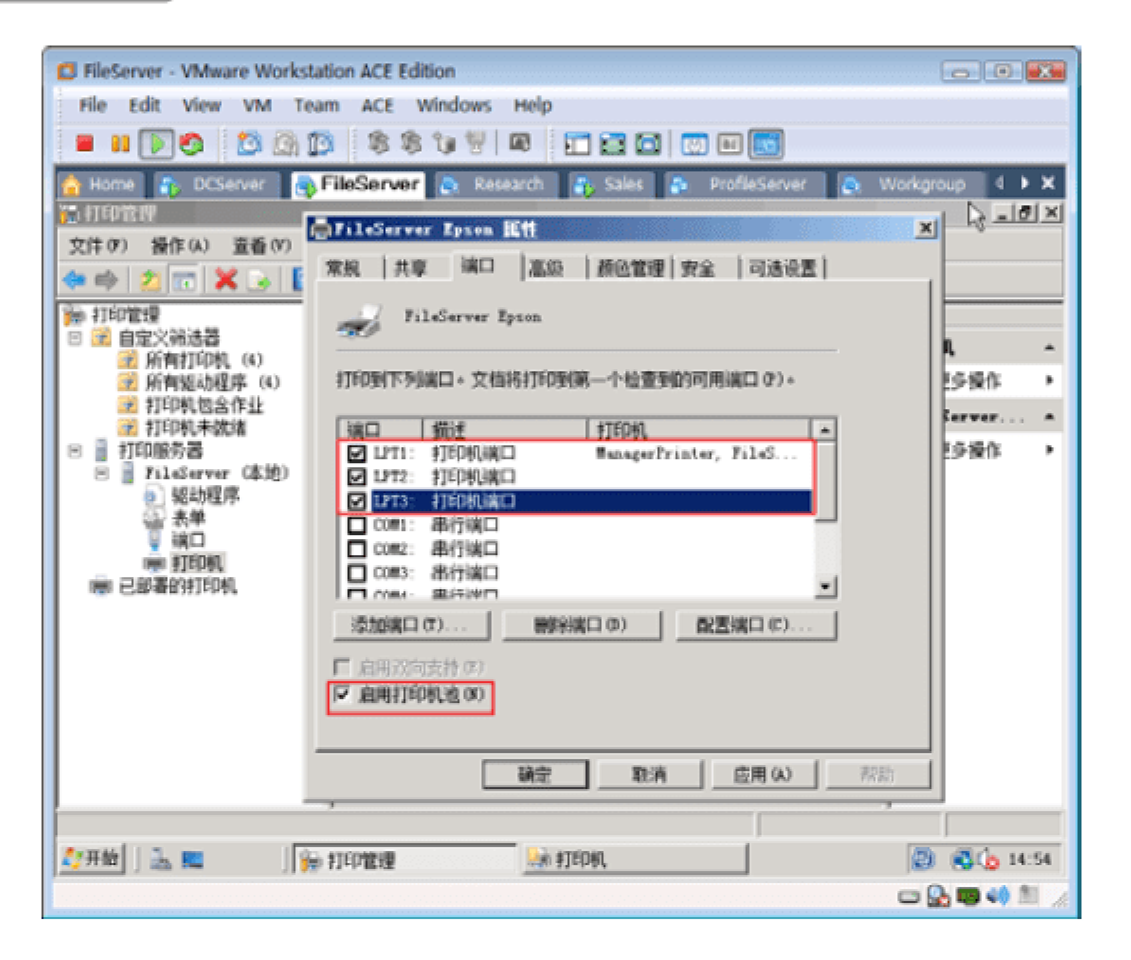


图 10-31　设置打印池

10.4.4　支持多种客户端

如果运行不同版本 Windows 的用户共享此打印机，则可能安装其他驱动程序。这样，当用户连接到共享打印机时就不需要查找打印驱动程序。

如图 10-32 所示，右击打印机，在弹出的快捷菜单中选择“属性”命令，在打开的打印机属性对话框的“共享”选项卡中，单击“其他驱动程序”按钮。在打开的对话框中选中 x64 和 Itanium 复选框，单击“确定”按钮，浏览到驱动盘，添加 x64 和 Itanium 驱动。

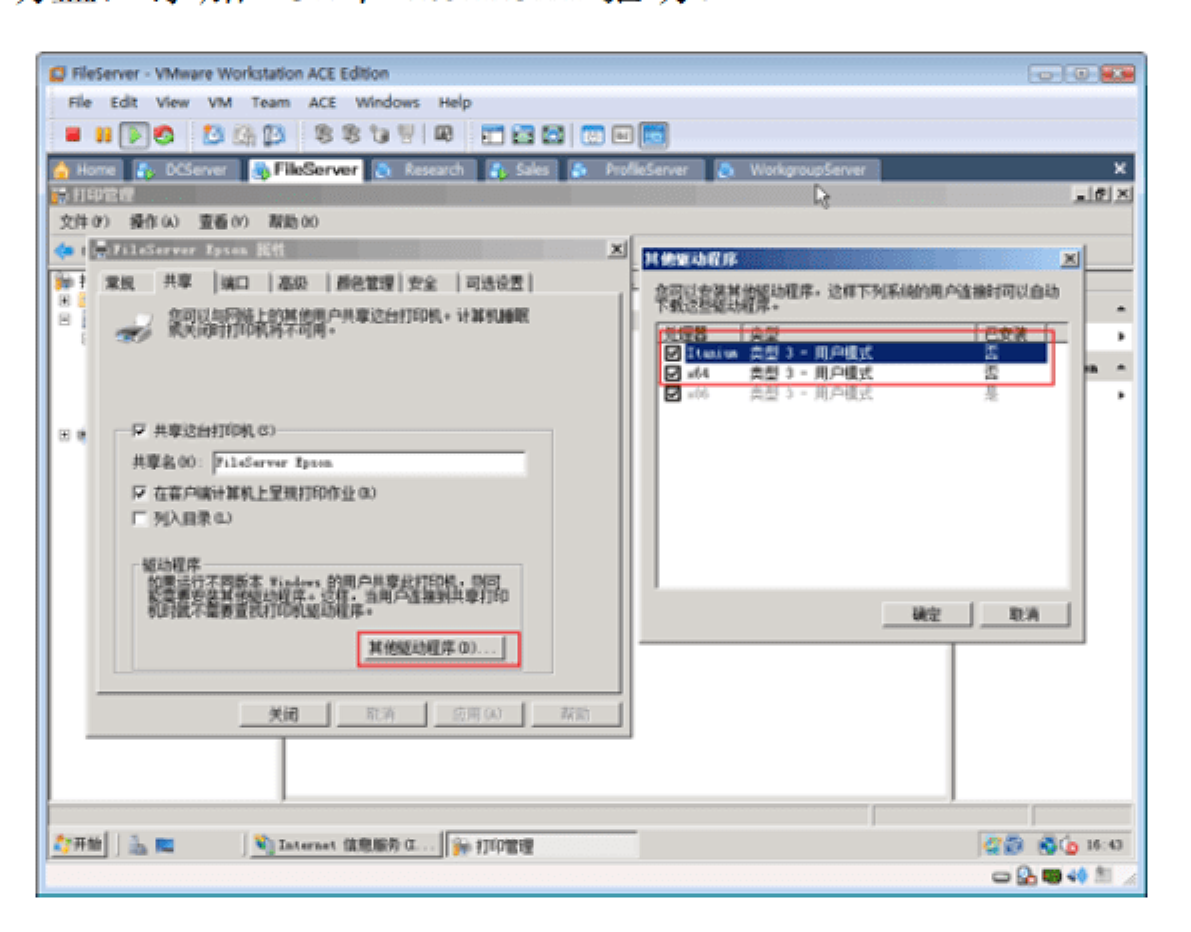


图 10-32　支持其他客户端

10.5　在域环境中部署打印机

本节介绍如何在域环境中部署打印机，如何使用组策略部署打印机。域用户一登录计算机就已经连接了网络管理员部署的网络打印机。

10.5.1　使用组策略自动部署打印机

例如，让销售部的用户一登录 Sales 计算机，就自动连接打印服务器上的 FileServer Epson 打印机。

以下步骤将使用组策略发布打印机，首先在 DCServer 上为销售部创建一个发布打印机的组策略，将打印服务器 FileServer 的打印机部署给销售部的用户。

① 以域管理员的身份登录 DCServer。

② 选择“开始”→“运行”命令，在打开的“运行”对话框中输入 gpmc.msc，单击“确定”按钮。

③ 如图 10-33 所示，选择“在这个域中创建 GPO 并在此处连接”命令，在出现的对话框中，输入组策略名称，单击“确定”按钮。

④ 如图 10-34 所示，在 FileServer 计算机上右击打印机，从弹出的快捷菜单中选择“使用组策略部署”命令。

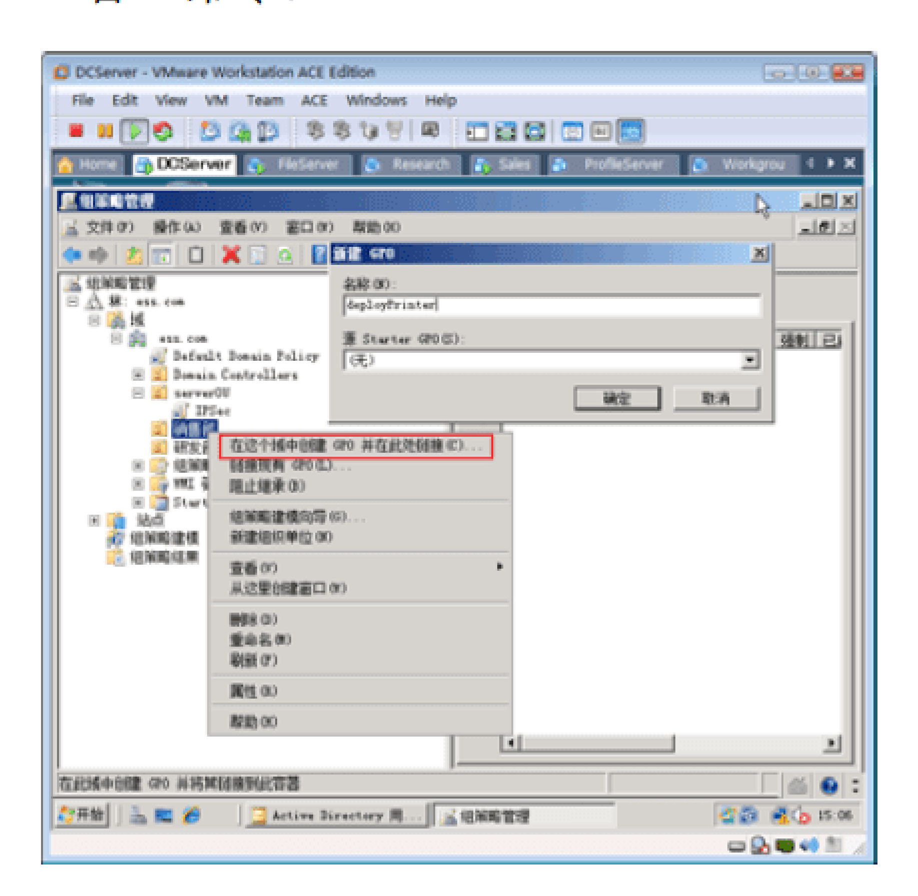


图 10-33　创建组策略

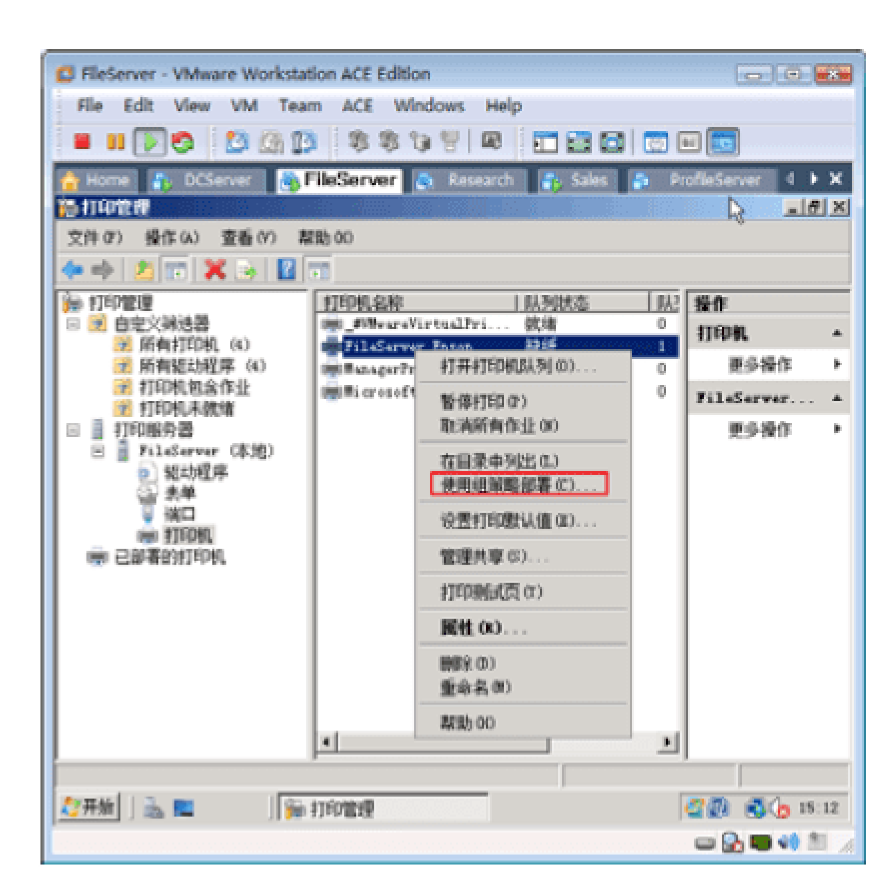


图 10-34　使用组策略部署打印机

⑤ 如图 10-35 所示，在出现的“浏览组策略对象”对话框中，单击“浏览”按钮，在出现的“浏览组策略对象”对话框中，选中 deployPrinter 组策略，单击“确定”按钮。

⑥ 如图 10-36 所示，在出现的“使用组策略部署”对话框中，选中“应用此 GPO 的用户(每位用户)”复选框，单击“添加”按钮。

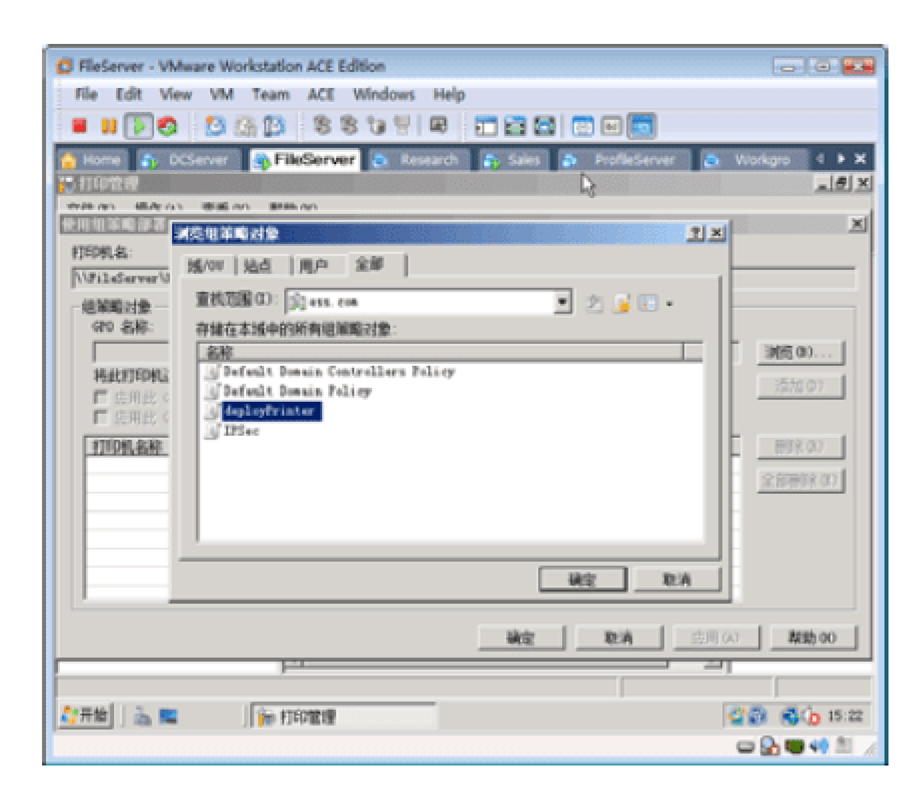


图 10-35　选择部署打印机的组策略

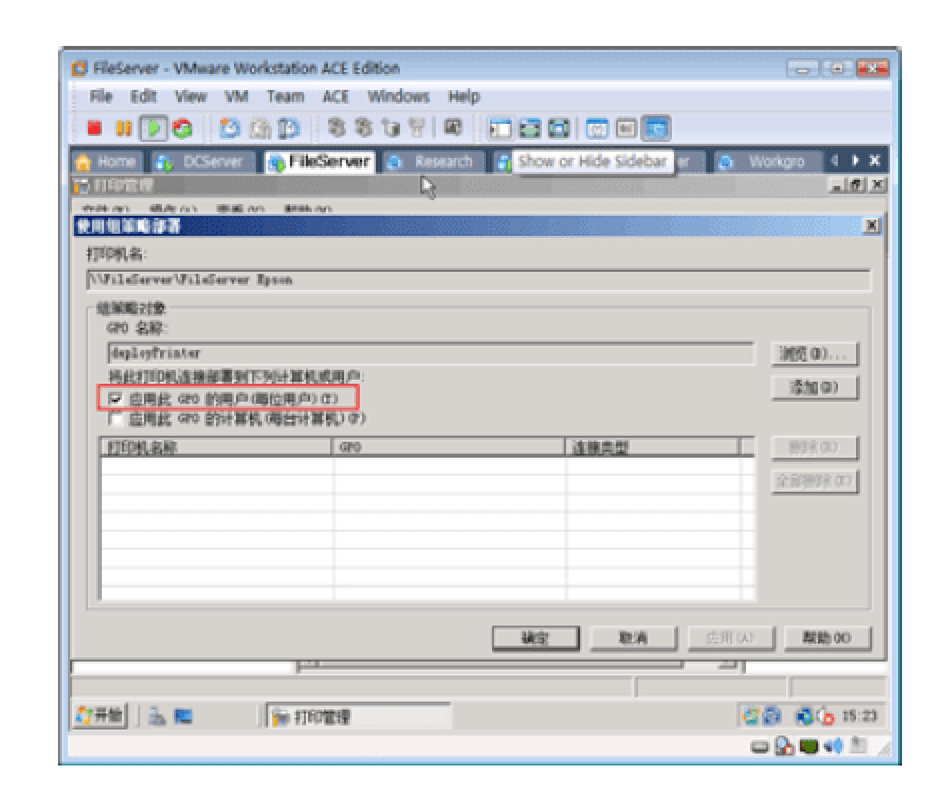


图 10-36　将打印机指定到用户

> **提示：** 选中“应用此 GPO 的用户(每位用户)”复选框，只要是销售部门的用户登录到域中任何计算机时，自动添加打印机。如果选中“应用此 GPO 的计算机(每台计算机)”复选框，销售部门的计算机只要一开机启动就自动连接打印机。

⑦ 如图 10-37 所示，在 Sales 计算机上删除以上任务添加的 FileServer 上的打印机。

⑧ 如图 10-38 所示，注销当前用户，使用销售部的用户 WangRS 登录。单击打印机，可以看到已经自动为用户连接好了网络打印机。

⑨ 如图 10-39 所示，使用域管理员登录，可以发现并没有自动为其连接网络打印机，因为域管理员账户不属于销售部门，登录时不应用部署打印机的组策略。

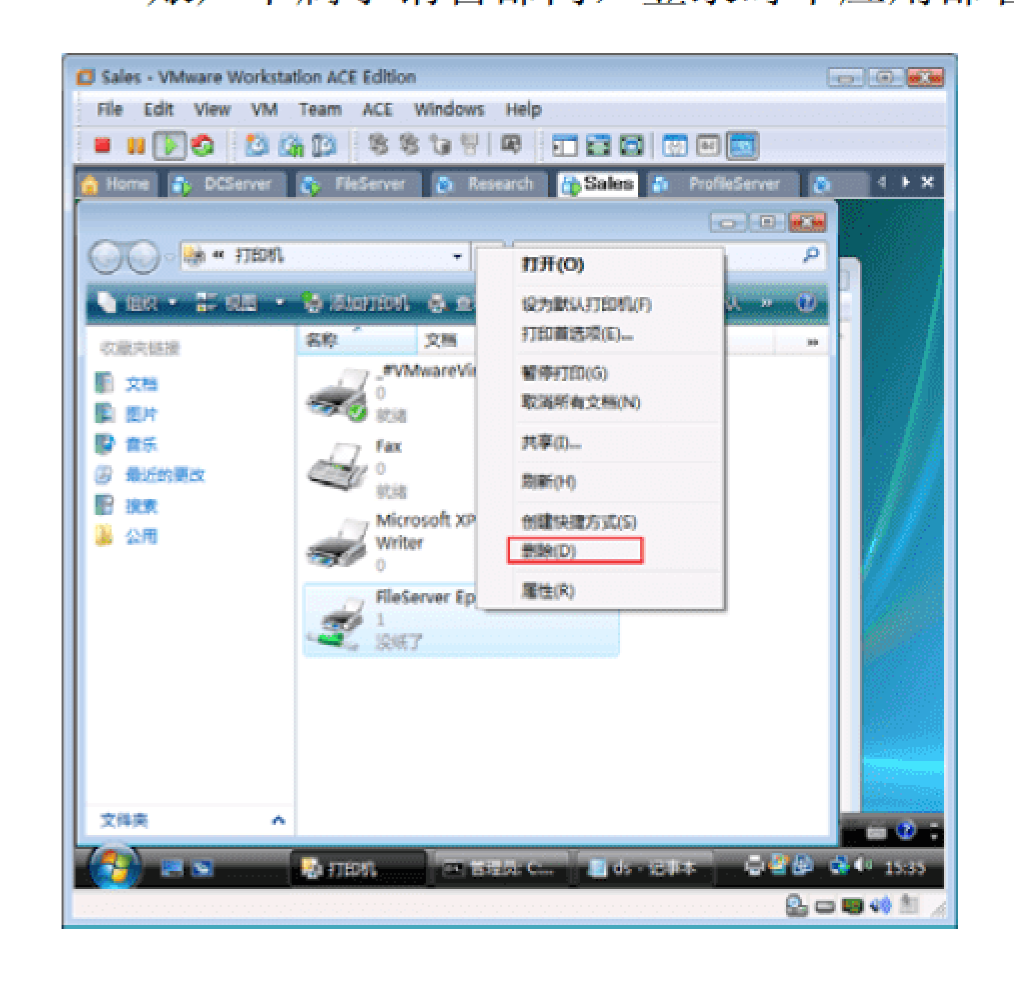


图 10-37 删除打印机

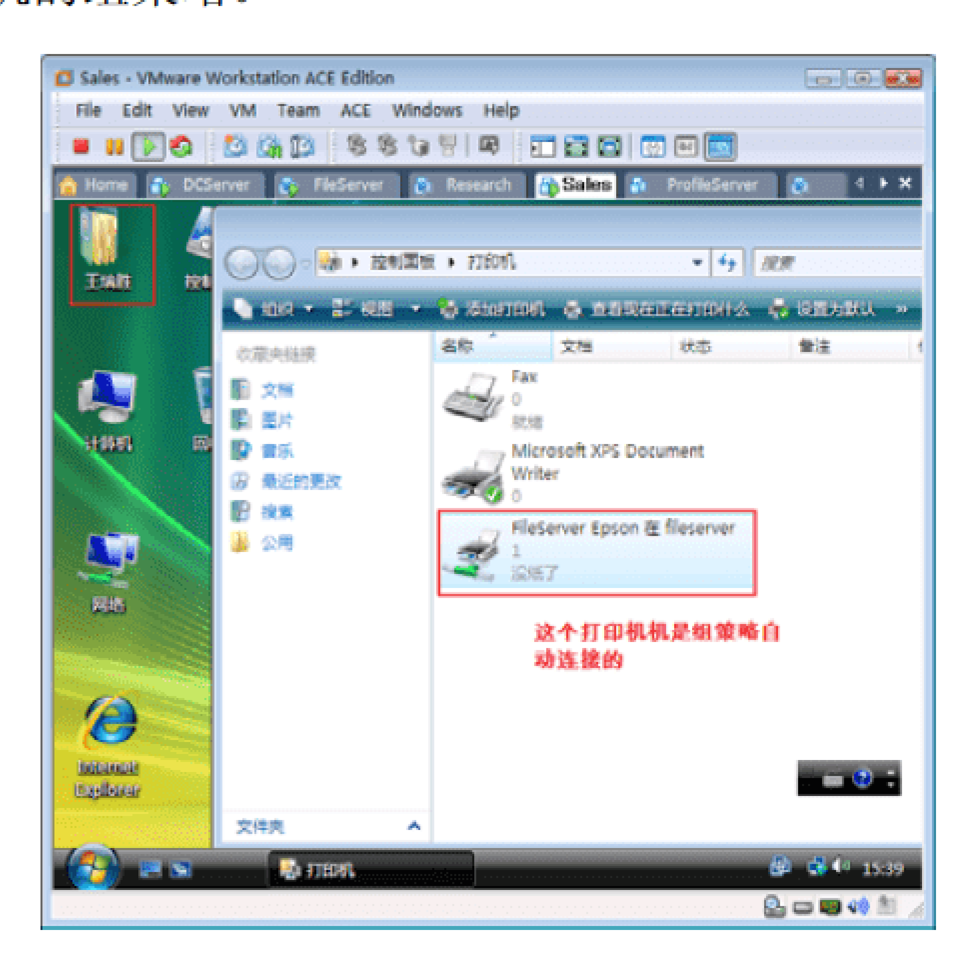


图 10-38 使用组策略部署的打印机

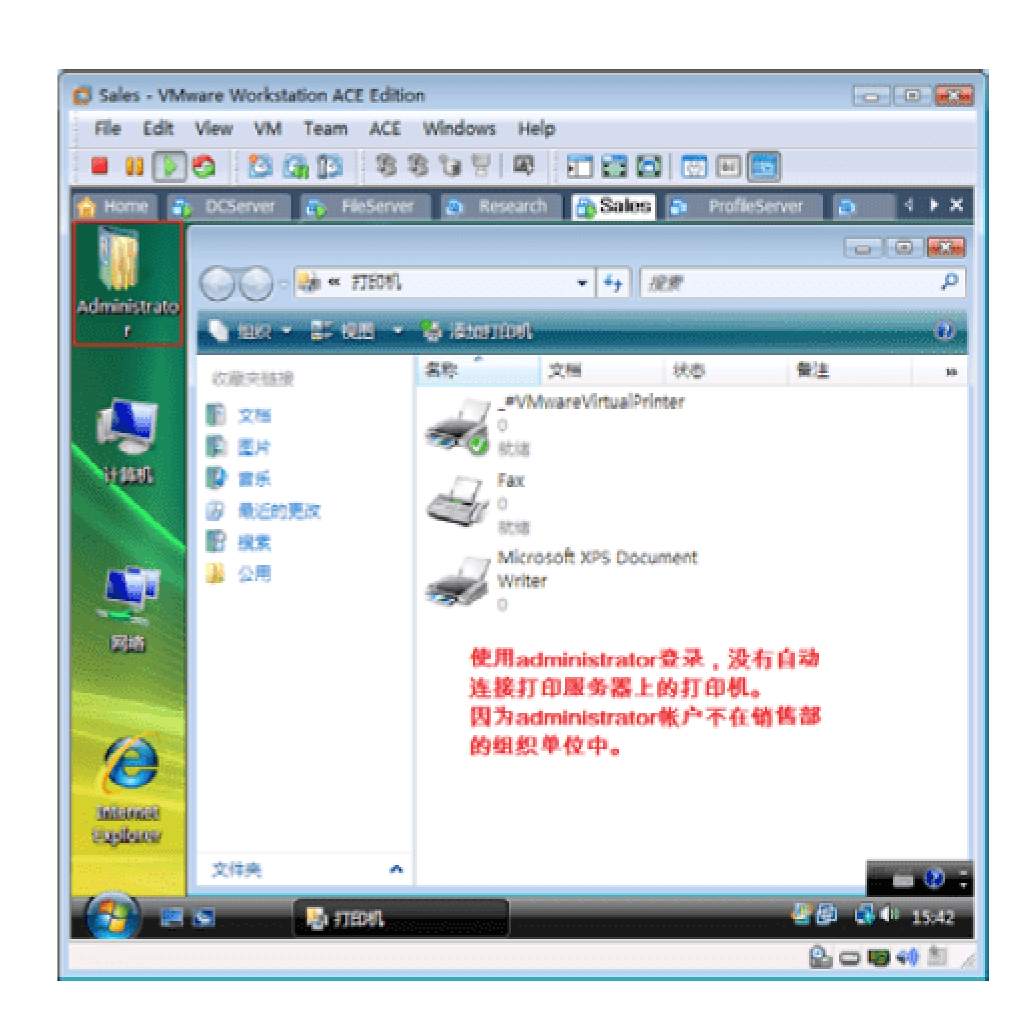


图 10-39 测试组策略部署的打印机

10.5.2 将打印机发布到活动目录中

为了使域中的用户方便查找打印机，管理员可以将打印服务器上的打印机列在活动目录中。域用户可

以方便地搜索列在活动目录中的打印机。

① 如图 10-40 所示，在打印服务器上，打开“打印管理”窗口，右击打印机，从弹出的快捷菜单中选择“在目录中列出”命令。

② 在 DCServer 上，选择“开始”→“运行”命令，在“运行”对话框中输入 dsa.msc，打开活动目录管理工具。

③ 如图 10-41 所示，右击 ess.com，从弹出的快捷菜单中选择“新建”→“组织单位”命令。

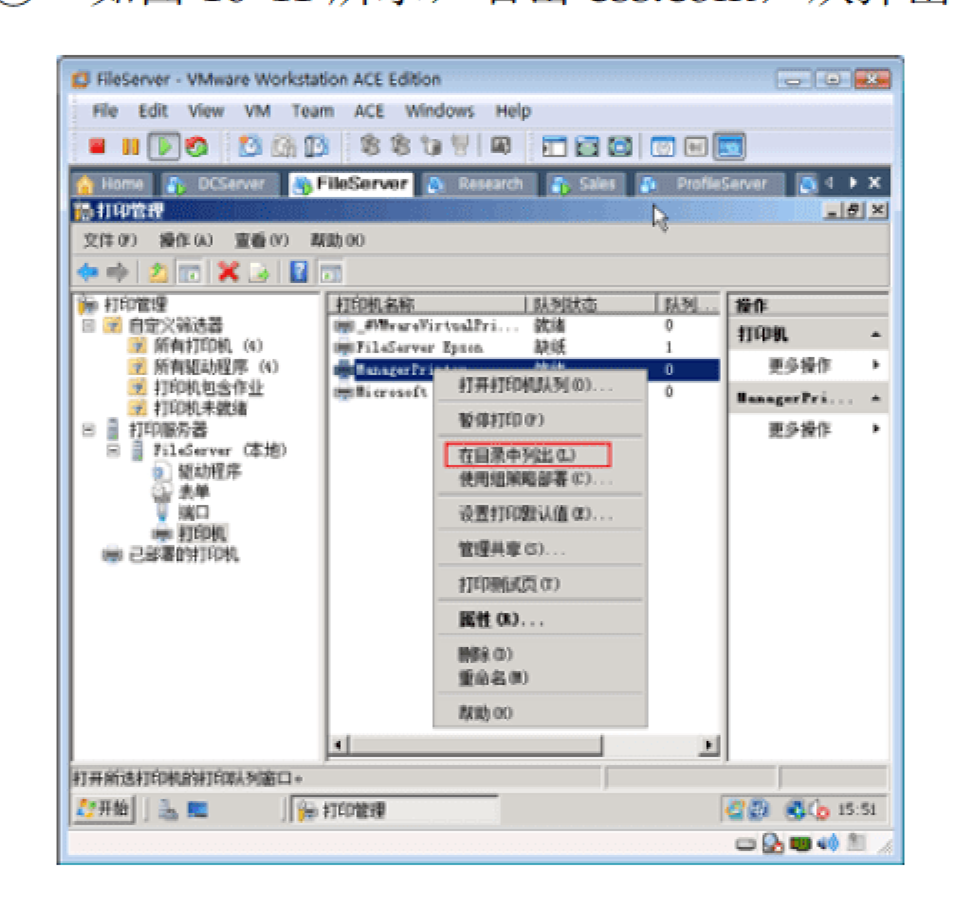


图 10-40　在目录中列出打印机

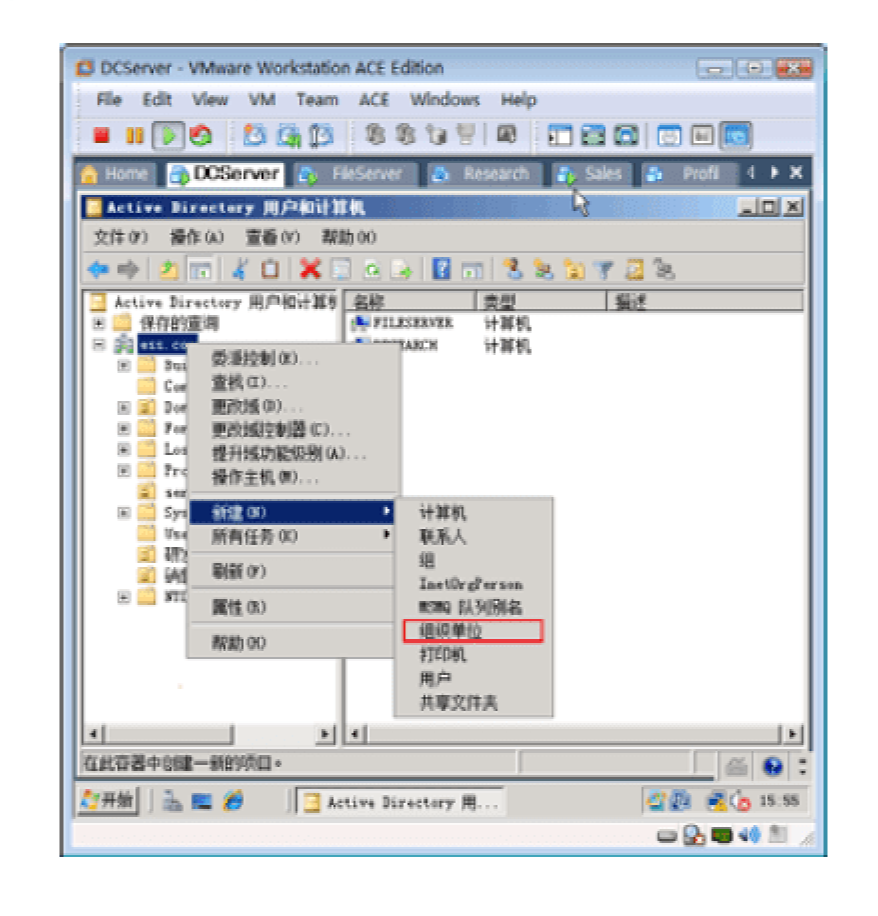


图 10-41　创建组织单位

④ 如图 10-42 所示，在出现的“新建对象”对话框中，输入组织单位名称 printersOU，单击“确定”按钮。

⑤ 如图 10-43 所示，选择“查看”→“用户、联系人、组和计算机作为容器”命令。

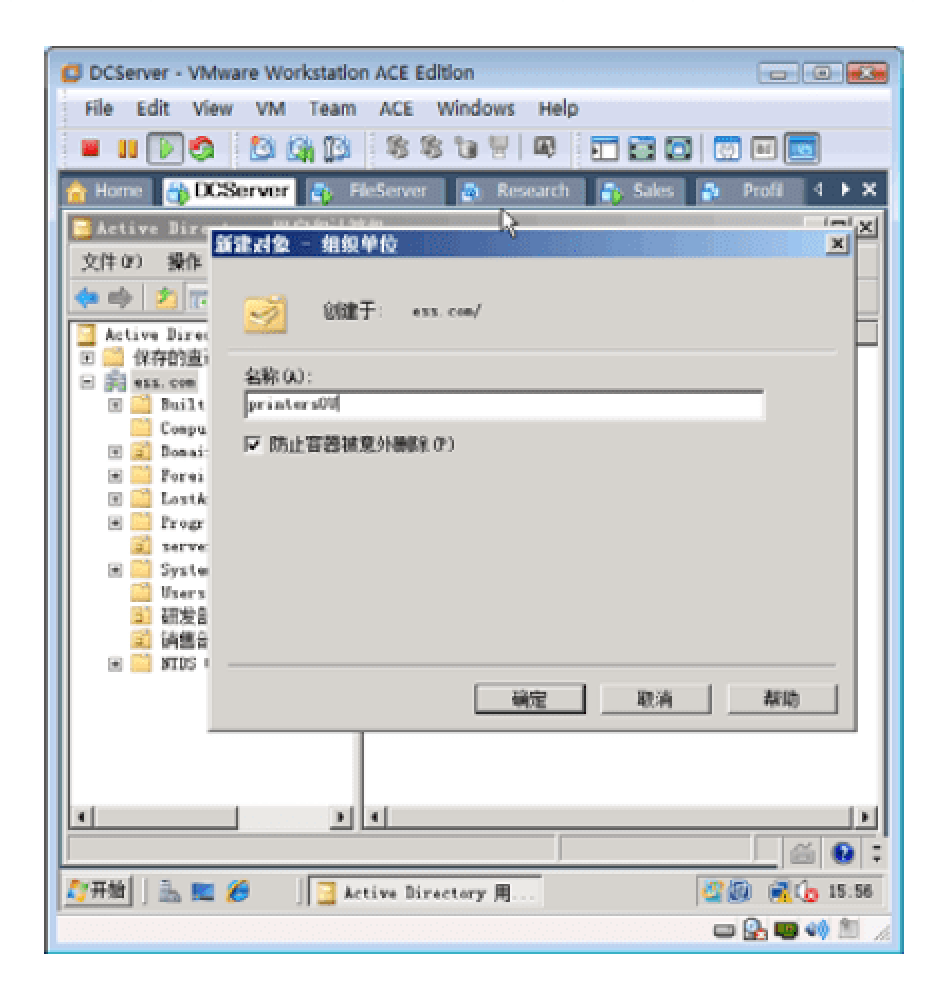


图 10-42　输入组织单位的名称

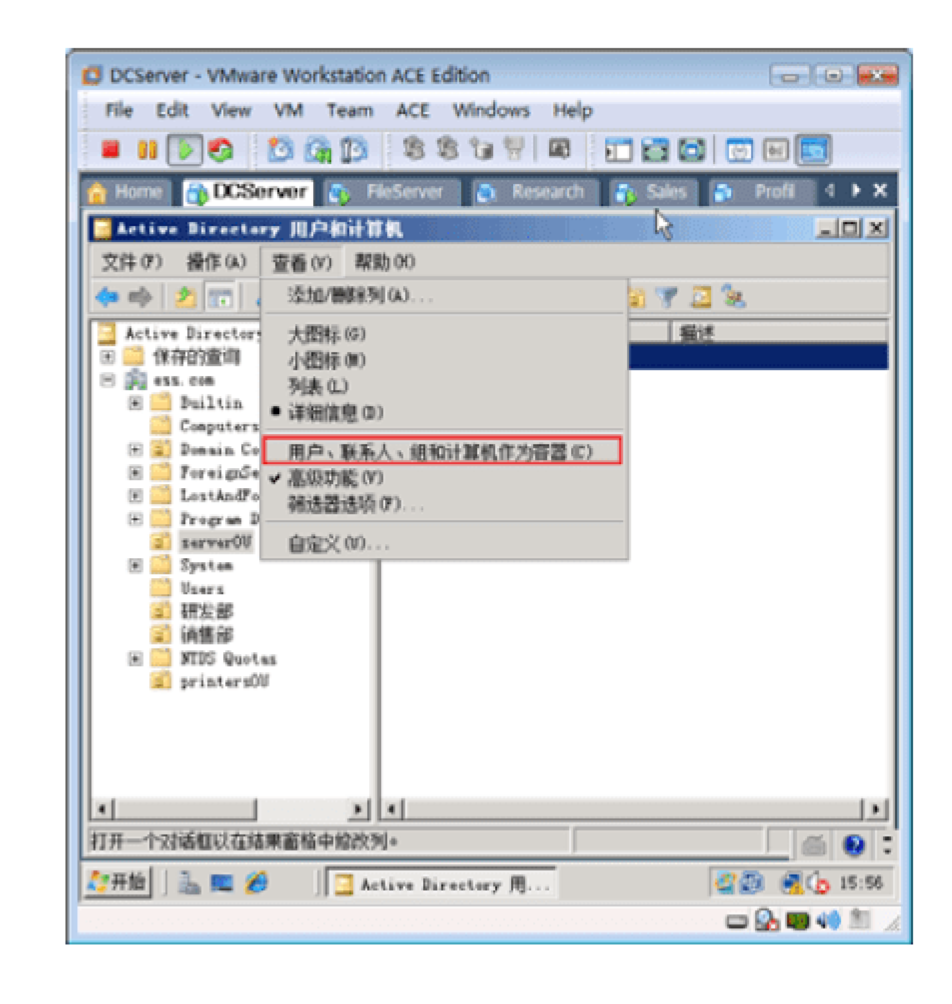


图 10-43　对象作为容器

⑥ 如图 10-44 所示，展开 ess.com→serverOU→FILESERVER 节点，右击打印机，从弹出的快捷菜单中选择“移动”命令。

⑦ 如图 10-45 所示，在出现的“移动”对话框中，选中 printersOU，单击“确定”按钮。

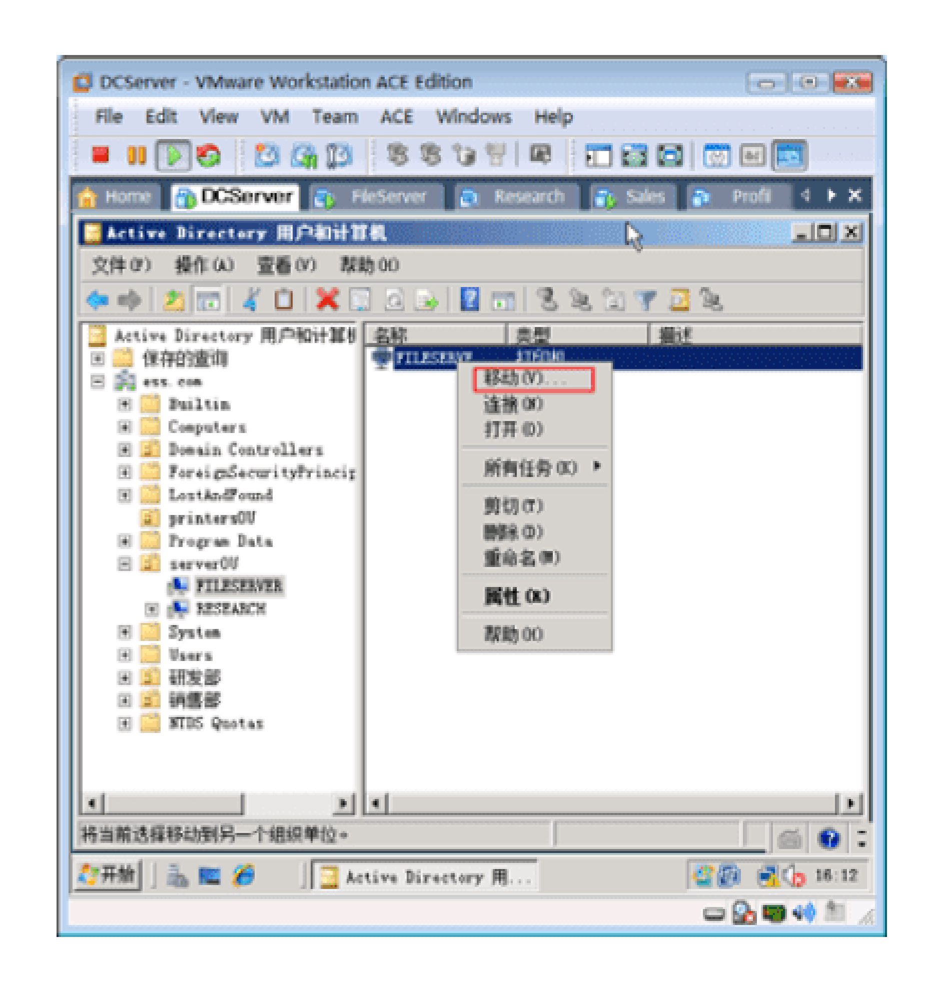




图 10-44　移动打印机(一)

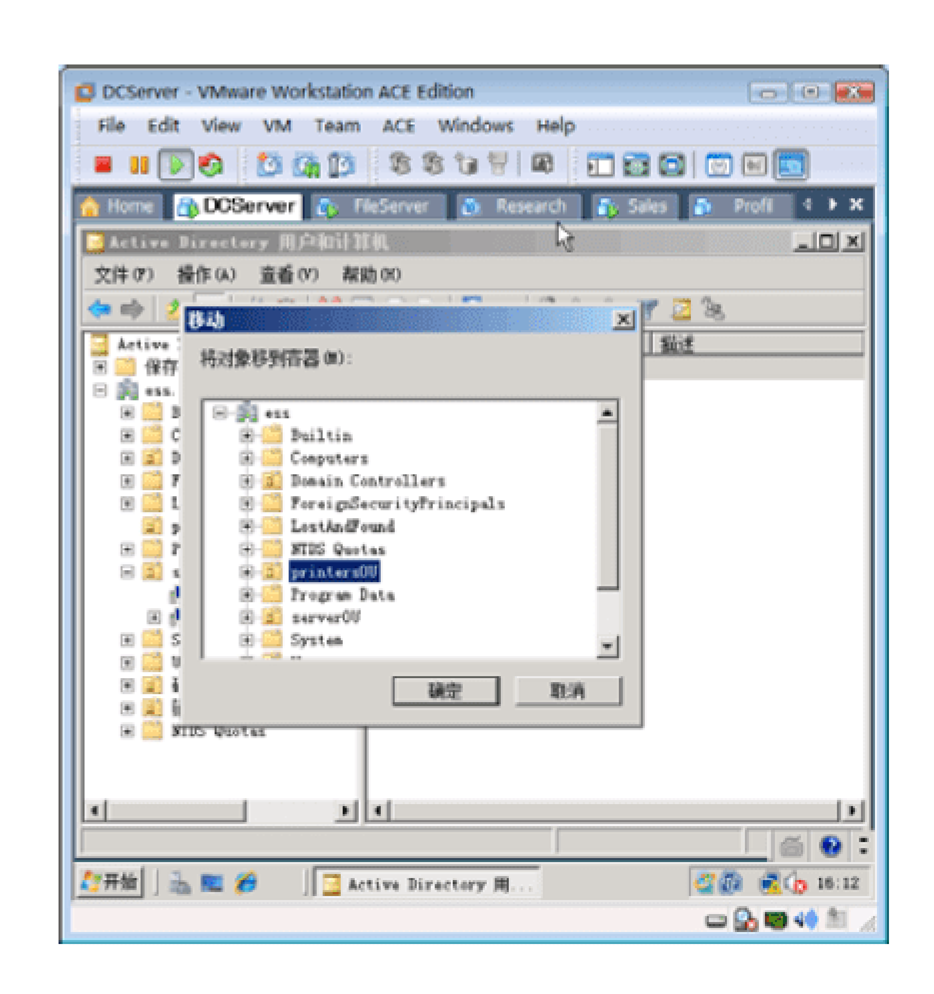


图 10-45　移动打印机(二)

⑧　可以看到打印机已经被移动到 printersOU。

⑨　如图 10-46 所示，在 Sales 计算机上，选择“开始”→“搜索”→“查找打印机”命令，在出现的“查找打印机”对话框中，单击“开始查找”按钮，可以列出发布在活动目录的打印机。右击打印机，从弹出的快捷菜单中选择“连接”命令，则可以连接到打印服务器上的打印机。

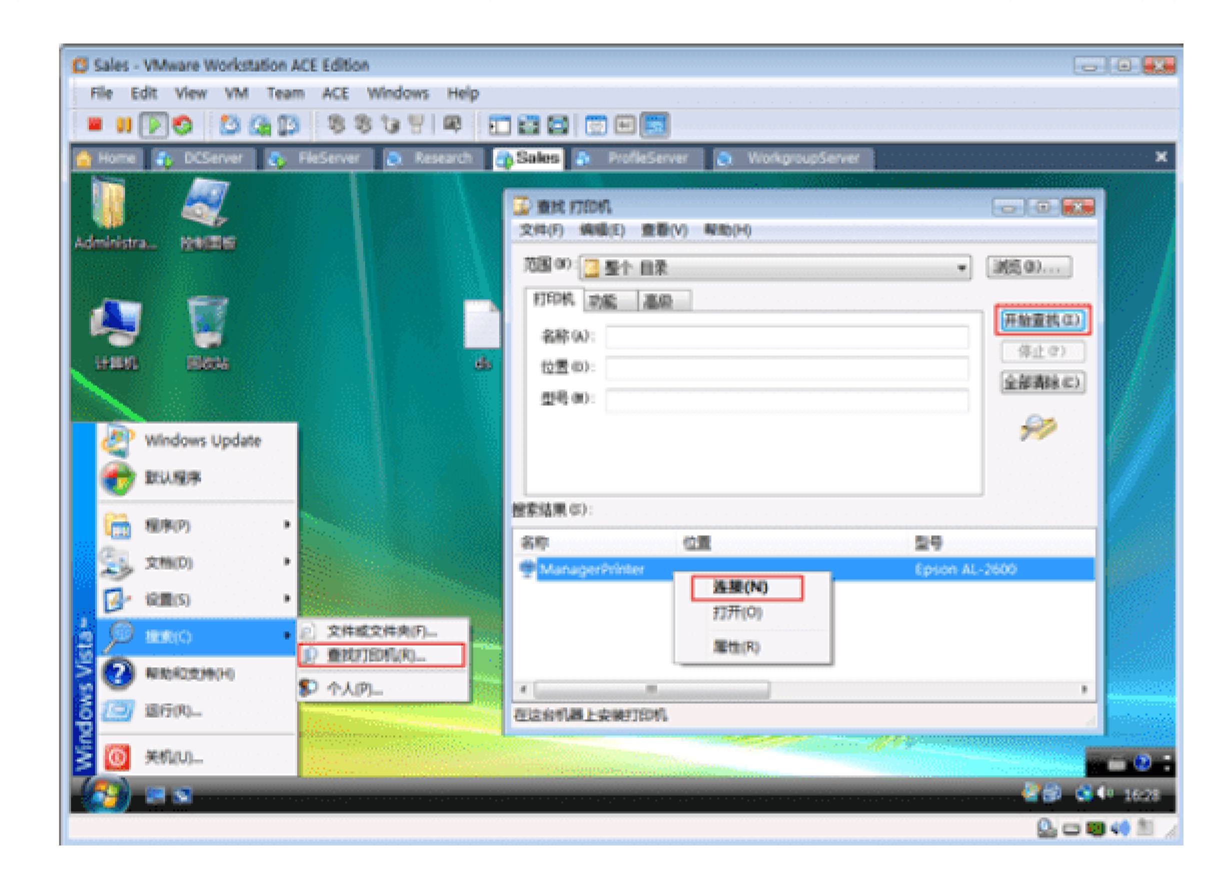


图 10-46　搜索活动目录中的打印机

10.6　配置 Internet 打印

■　使用 Internet 打印机，远程用户可以通过 TCP 的 80 端口将打印作业发送到打印服务器。但必须完成以下操作。

- 客户必须是域中的计算机。
- 必须使用域管理员在客户端添加 Internet 打印机。
- 添加的 Internet 打印机在客户端对任何用户可用。
- 在连接 Internet 打印机时，打印服务器的打印机硬件必须连接好。

- 确保用户在企业内部连接时用的 URL 在 Internet 上也能解析到打印服务器。

■ 安装 Internet 打印，如图 10-47 所示，打开“添加角色向导”对话框的“选择角色服务”界面，单击“打印服务”下面的“角色服务”，选中“打印服务器”和“Internet 打印”复选框，完成安装。



图 10-47　安装 Internet 打印

检查打印服务器是否已经配置好了对 Internet 打印的支持。

① 在 FileServer 服务器上，选择“开始”→“程序”→“管理工具”→“Internet 信息服务(IIS)管理器”命令。

② 如图 10-48 所示，展开“网站”→Default Web Site→Printers 节点，单击“浏览*:80(http)”按钮。

③ 如图 10-49 所示，在浏览器中能够看到打印服务器上共享的打印机。说明打印服务器支持 Internet 打印。

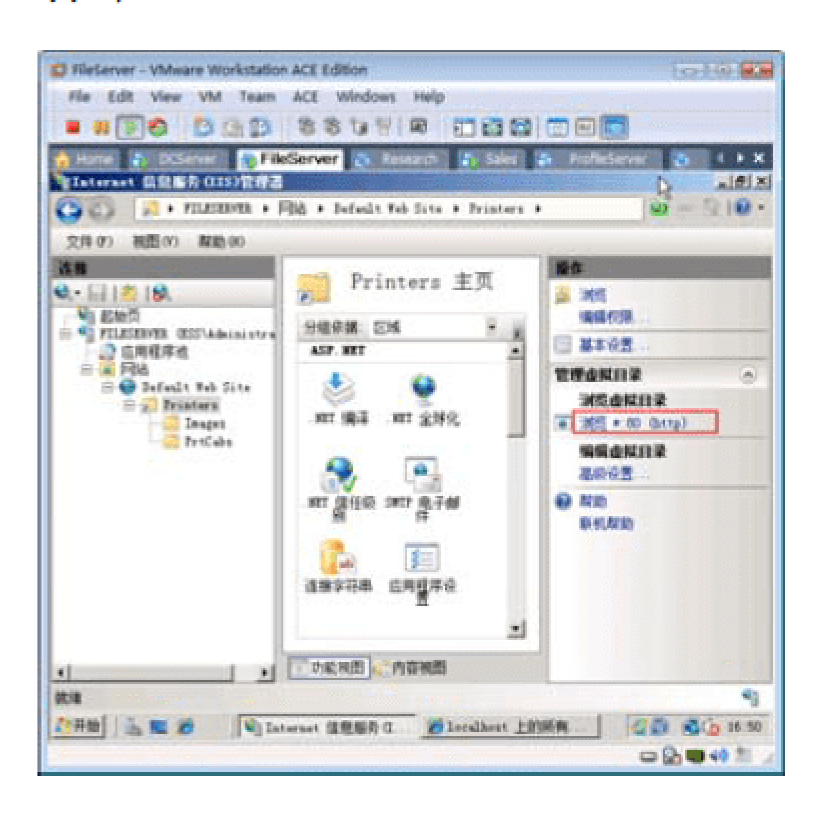


图 10-48　浏览 Printers 目录

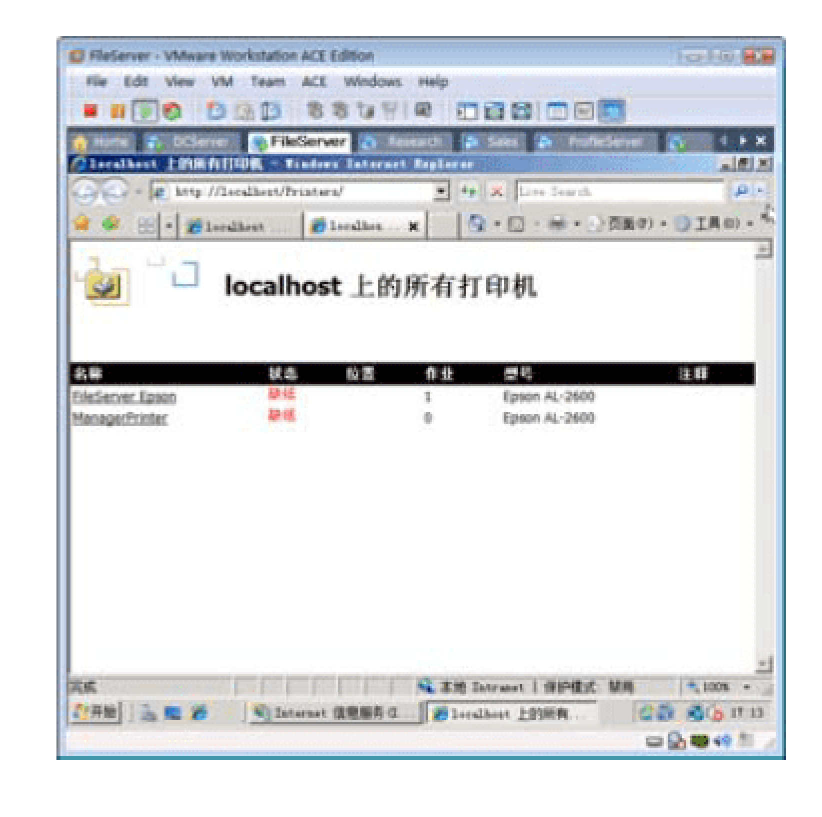


图 10-49　查看打印服务器上的打印机

④ 在 Sales 计算机上，以域管理员账户登录。

⑤ 选择“开始”→“设置”→“控制面板”→“程序和功能”命令，在出现的对话框中单击“打开或关闭 Windows 功能”按钮。

⑥ 如图 10-50 所示，在出现的对话框中，确保“Internet 打印客户端”复选框已经选中。



注意：Vista 默认已经安装了 Internet 打印客户端。Window Server 2008 必须安装 Internet 客户端功能才能连接 Internet 打印机。

⑦ 如图 10-51 所示，右击 IE，在弹出的快捷菜单中选择“属性”命令。在“Internet 属性”对话框的“安全”选项卡中，单击“可信站点”按钮，将安全级别调至最低，单击“站点”按钮。

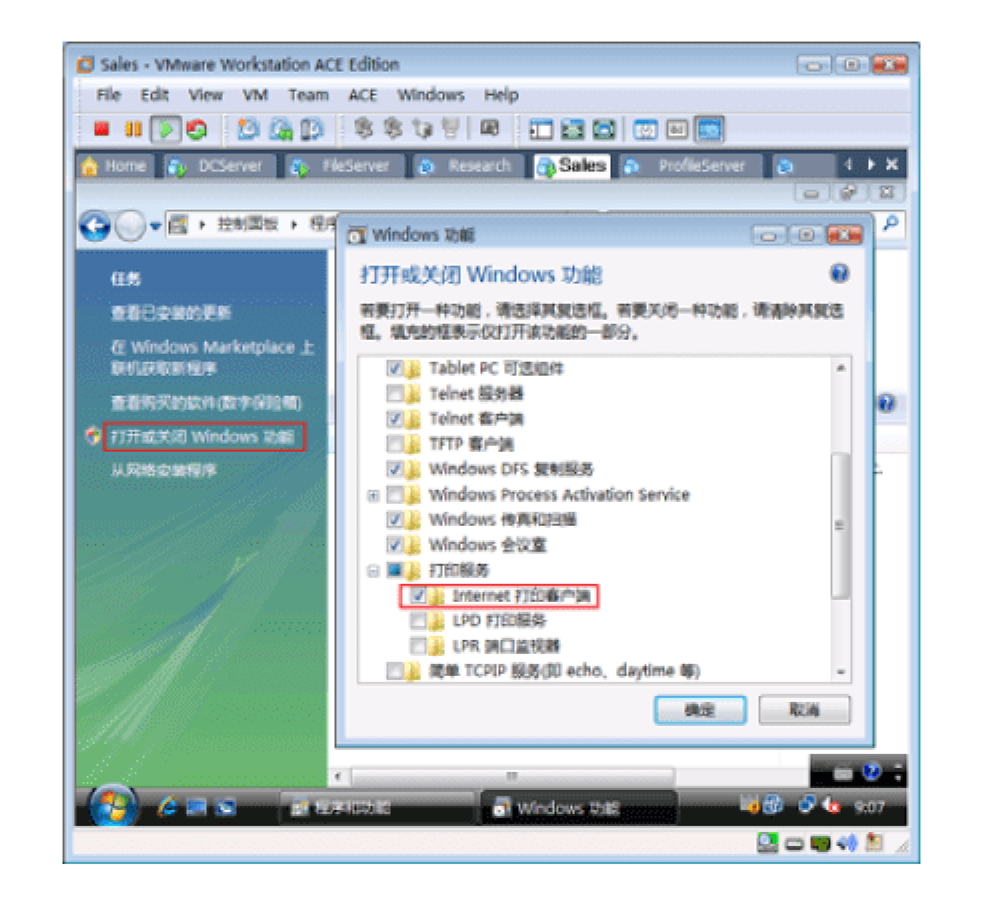


图 10-50 安装 Internet 打印客户端

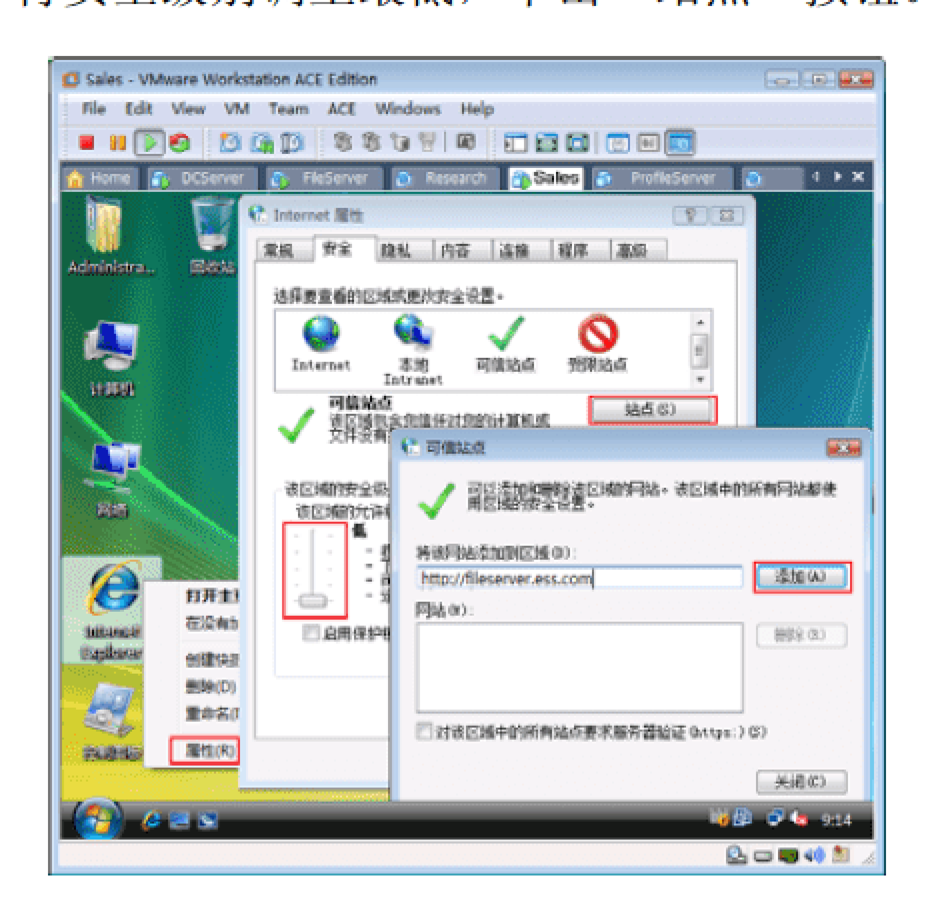


图 10-51 将打印服务器的 URL 添加到可信站点

⑧ 如图 10-51 所示，在“可信站点”对话框中输入 http://fileserver.ess.com，单击“添加”按钮。

注意：因为要通过网站下载打印驱动，所以需要将可信站点的安全级别降至最低，并将打印机的网址添加到受信站点。

⑨ 如图 10-52 所示，选择“开始”→“设置”→“打印机”命令，单击“添加打印机”按钮，在出现的添加打印机对话框中，单击“添加网络、无线或 Bluetooth 打印机”按钮。

⑩ 如图 10-53 所示，在出现的对话框中，单击“我需要的打印机不在列表中”按钮。

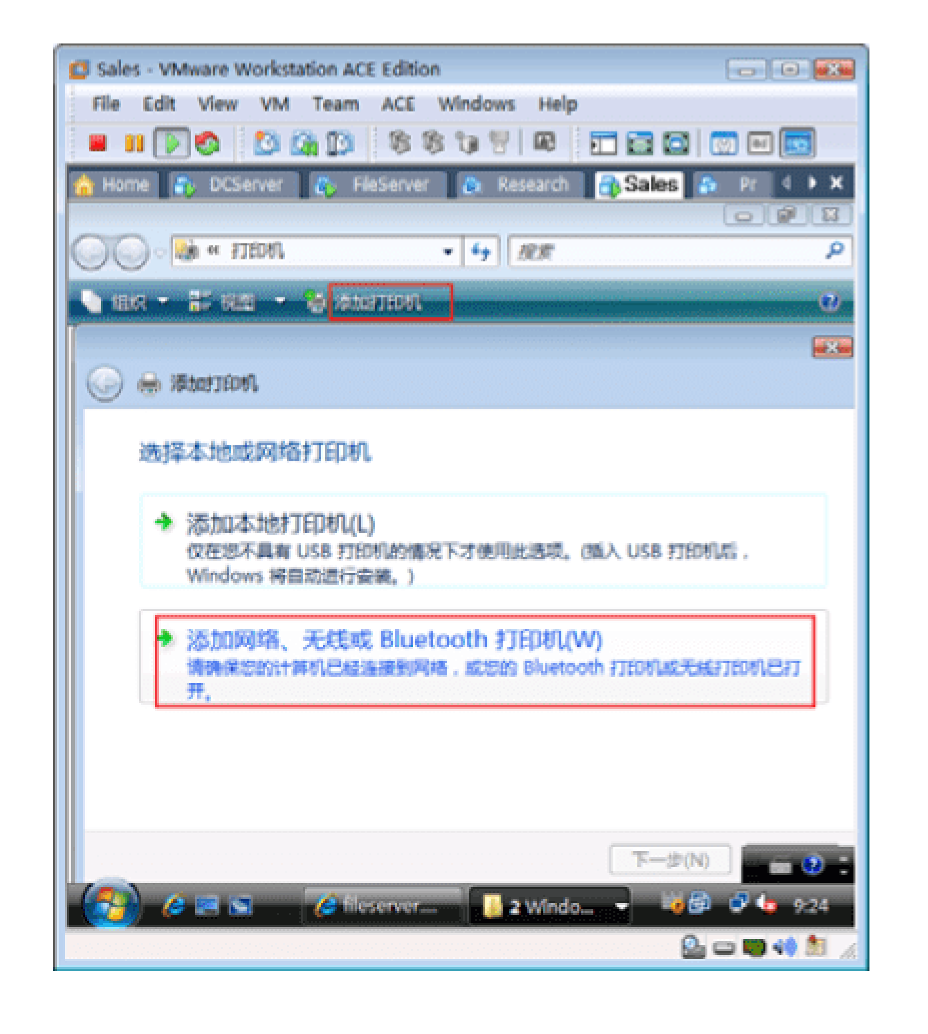


图 10-52 添加网络打印机

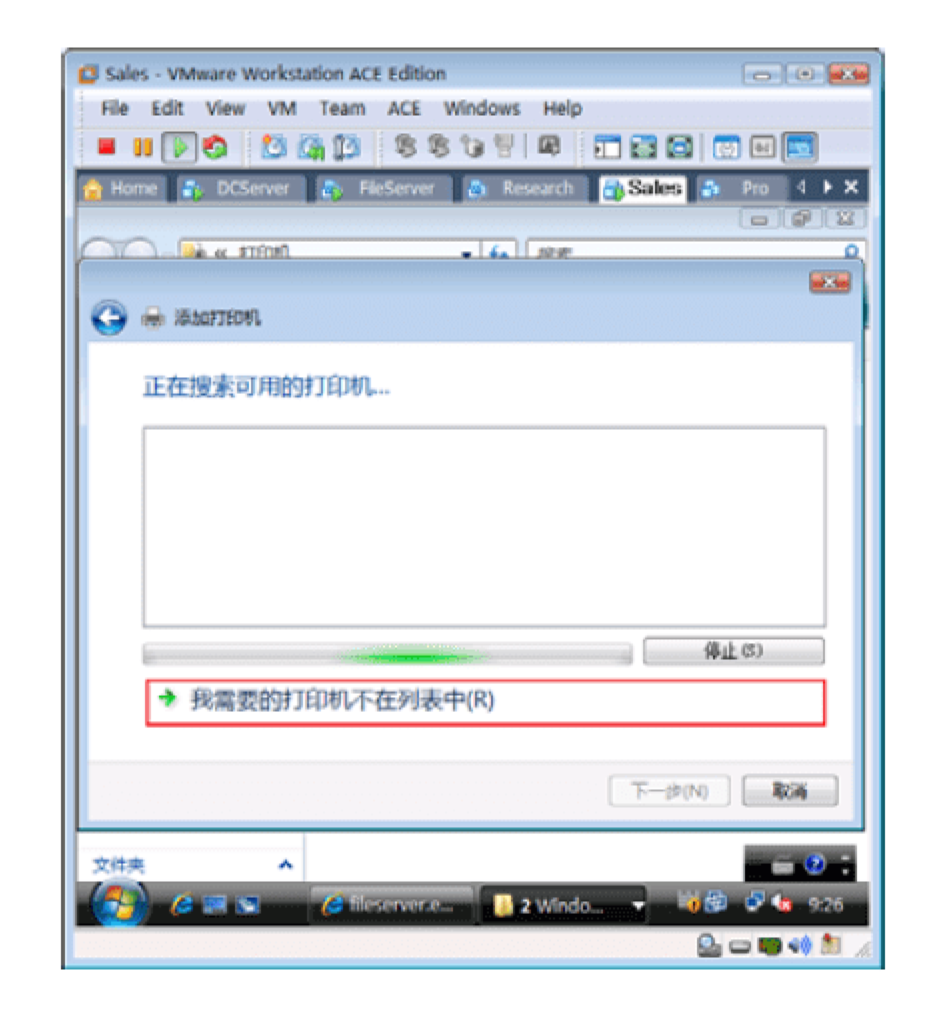


图 10-53 搜索打印机

⑪ 如图 10-54 所示，在出现的对话框中，单击“按名称选择共享打印机”单选按钮，并在下面的文本框中输入 http://fileserver.ess.com/printers/hp/.printer，单击“下一步”按钮。

注意： 该 URL 中，fileserver.ess.com 是打印服务器的域名，该域名在 Internet 上必须能够解析到打印服务器的 IP 地址。hp 是打印服务器上打印机共享的名称。其他都是固定格式。

⑫ 如图 10-55 所示，单击“从磁盘安装”按钮。在出现的对话框中单击“浏览”按钮，定位到驱动程序的文件夹。

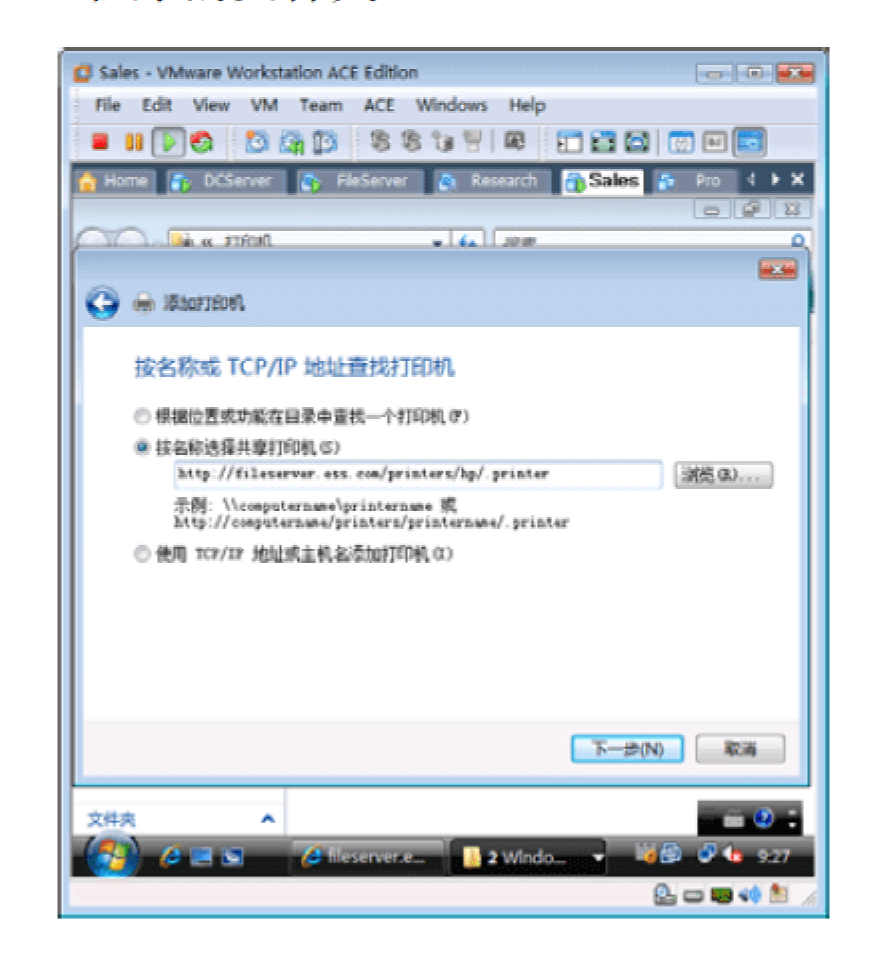




图 10-54 输入打印机名称

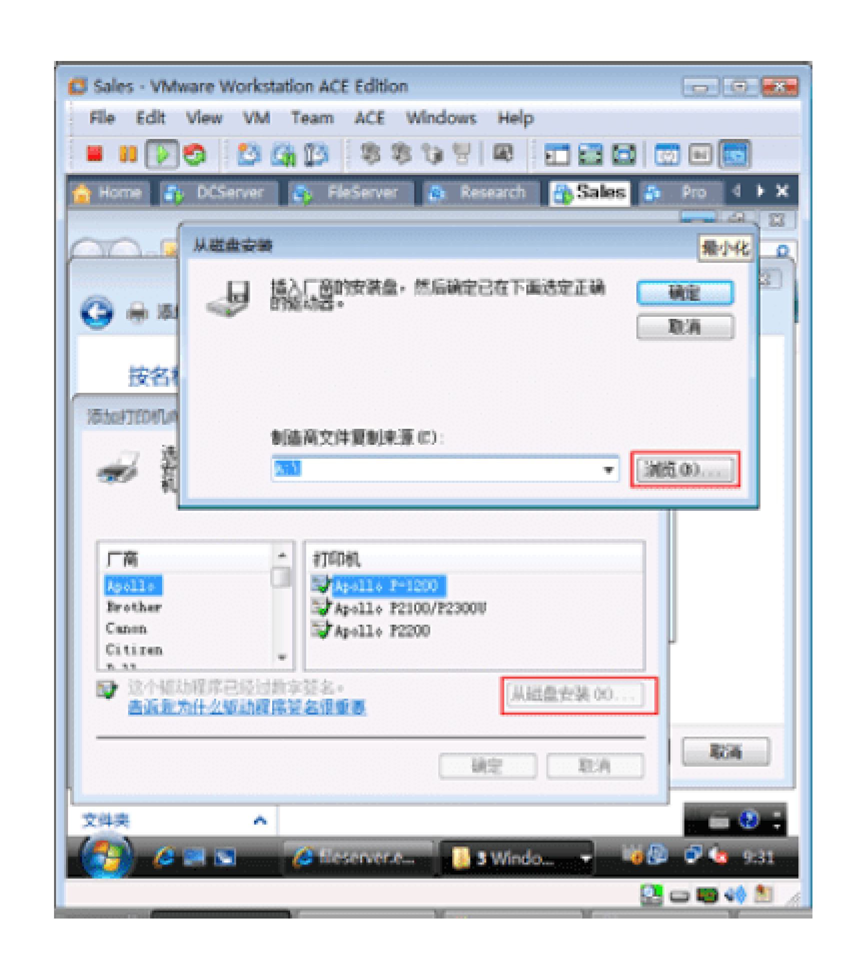


图 10-55 选择打印机型号和驱动

⑬ 如图 10-56 所示，选中 HP LaserJet 1000 打印机，单击“确定”按钮。

⑭ 如图 10-57 所示，在出现的打印机名称对话框中单击“下一步”按钮，完成打印机的添加。

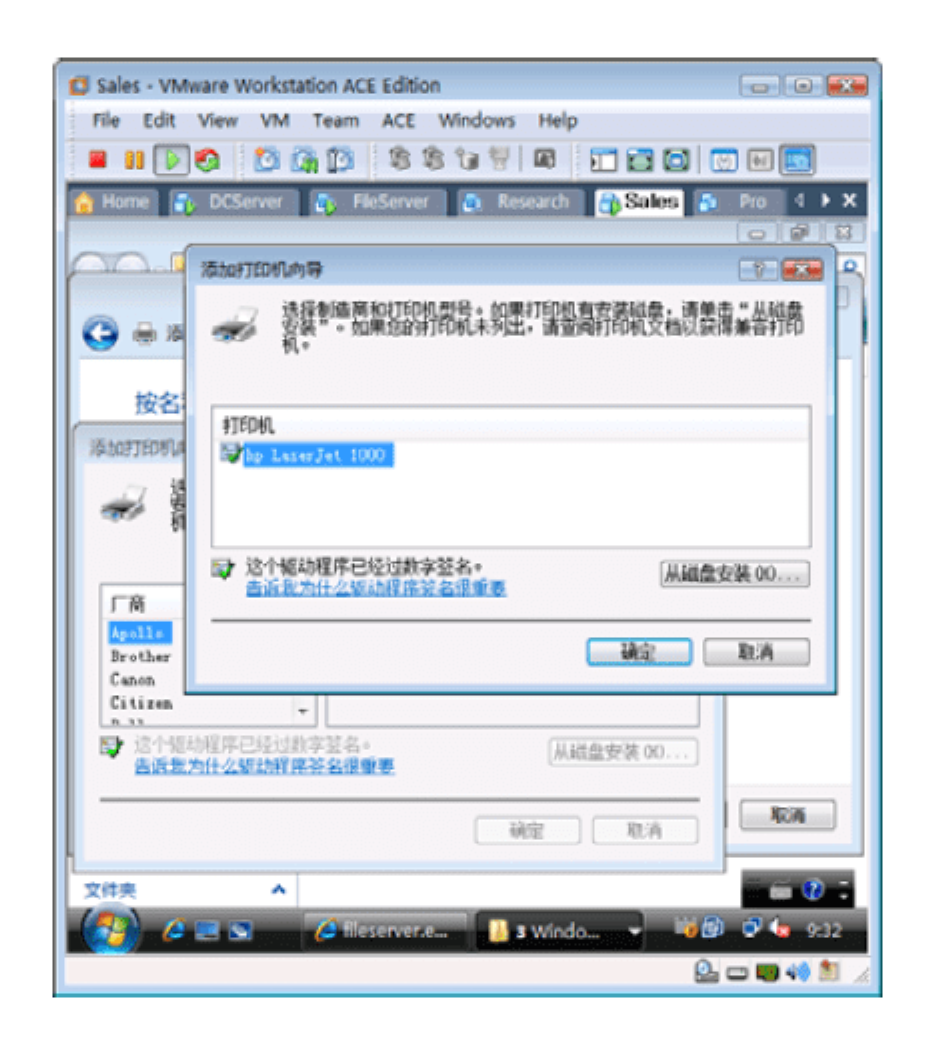


图 10-56 选择打印机

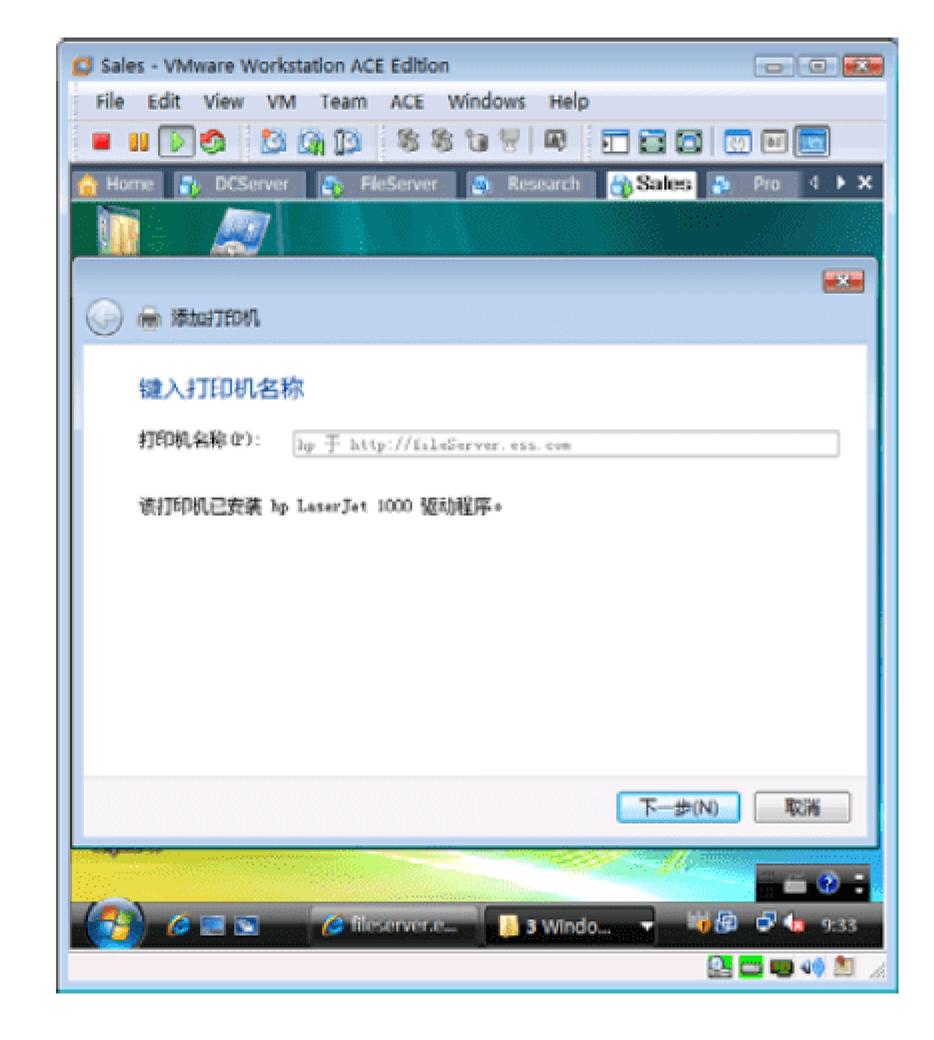


图 10-57 打印机名称

⑮ 如图 10-58 所示，可以看到已经添加了一个网络打印机。发送一个打印作业给打印服务器。

⑯ 如图 10-59 所示，输入 http://fileserver.ess.com/printers。单击 hp 可以看到与该打印机相关的打印作业。

⑰ 如图 10-60 所示，单击“文档列表”，可以看到打印作业，可以暂停选中的作业，或者取消、继续打印作业。

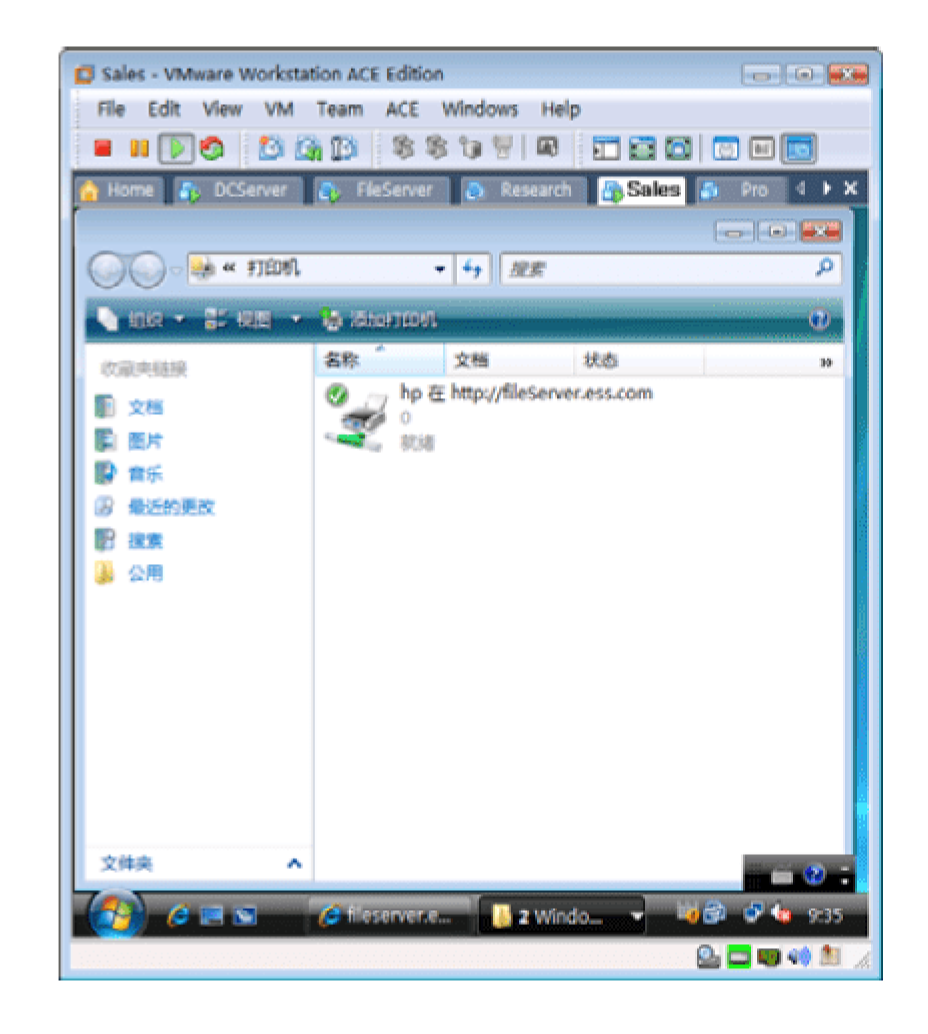


图 10-58　连接的 Internet 打印机

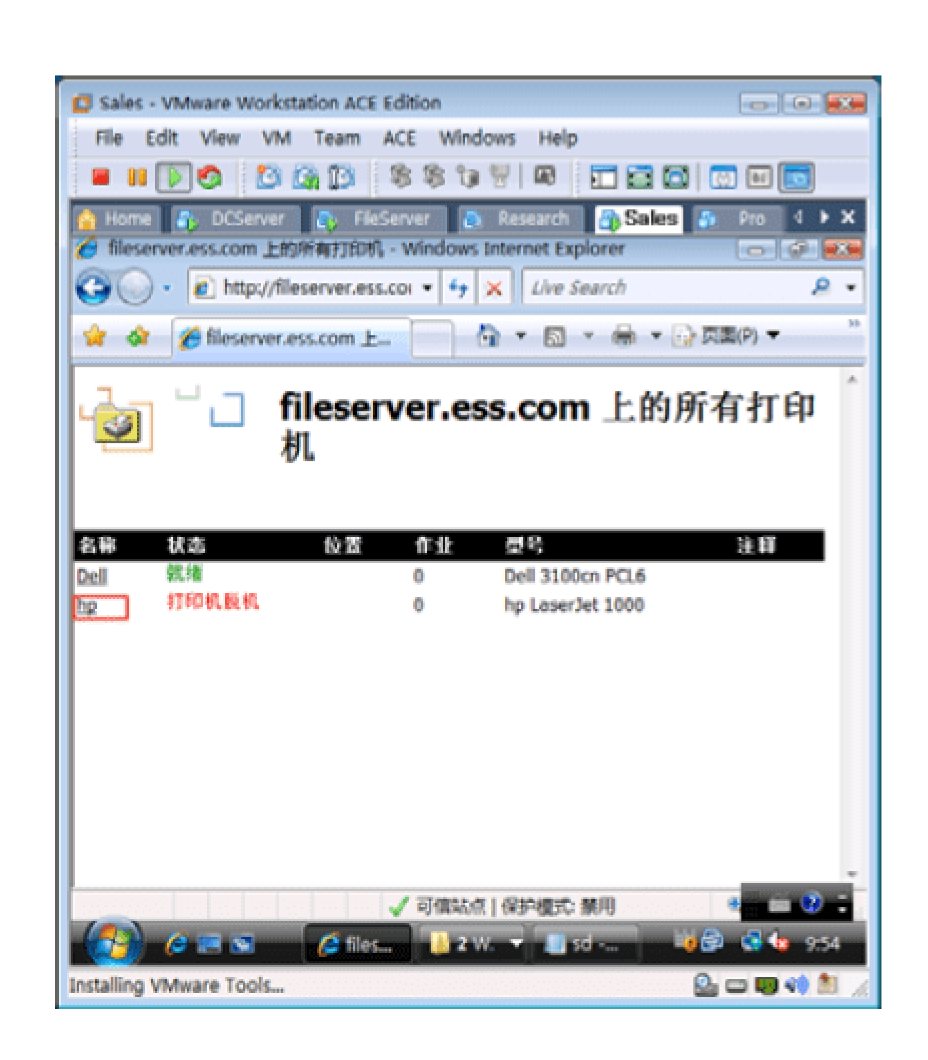


图 10-59　查看打印机状态

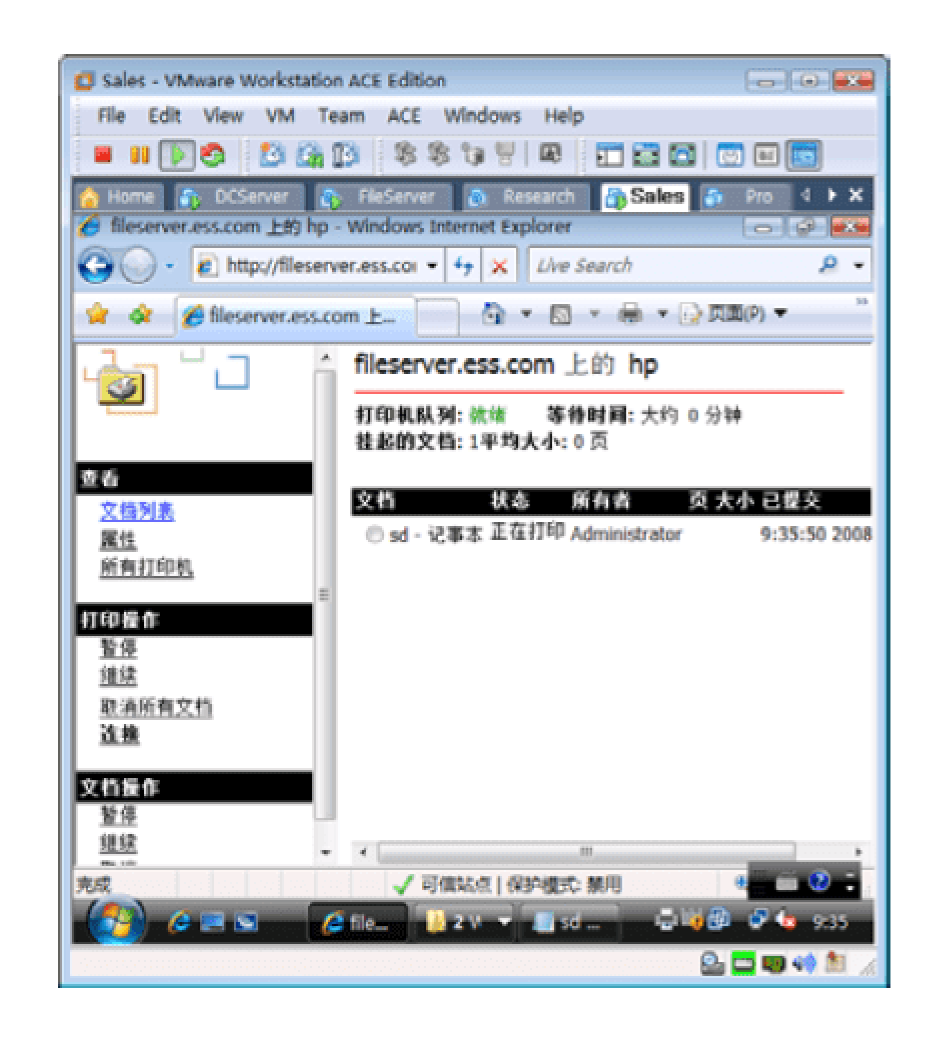


图 10-60　管理打印作业

10.7　Windows Server Core 作为打印服务器

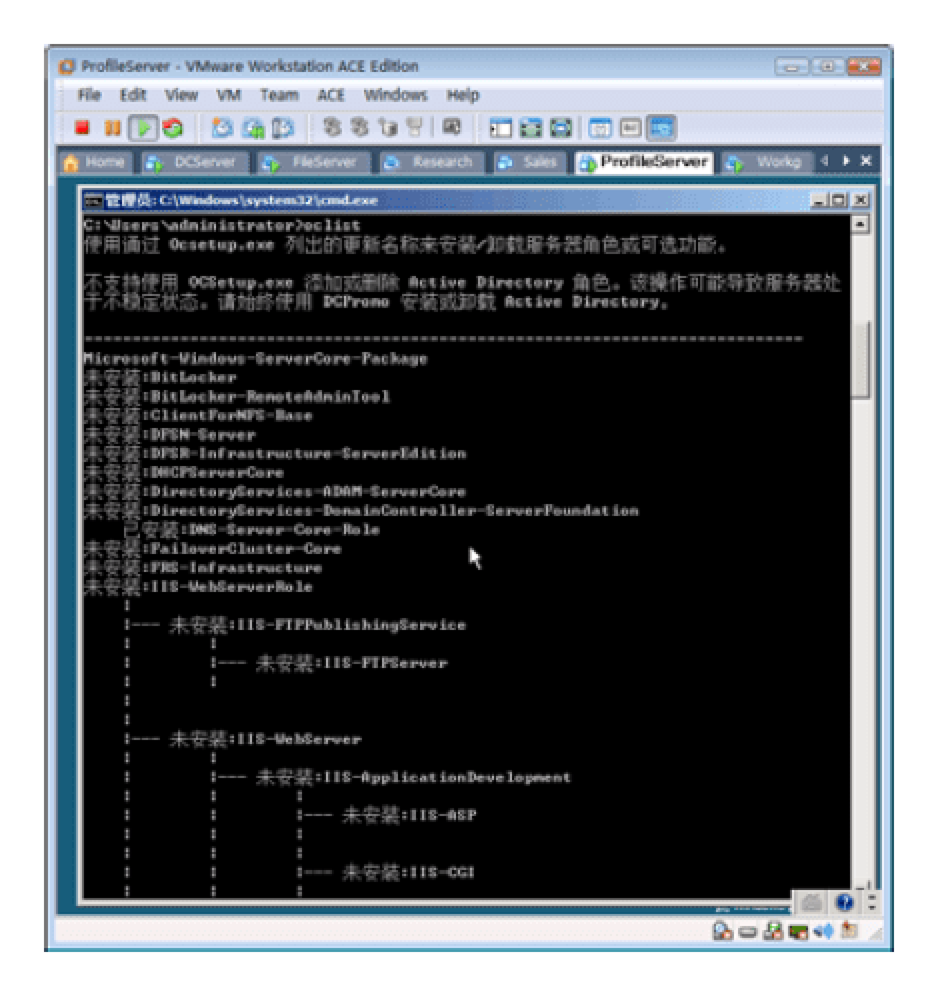
Windows Server Core 是 Windows Server 2008 的一种安装模式，其特点就是安装完以后没有图形化界面，登录界面与普通模式相同。但登录以后，你会发现桌面上没有开始菜单，也没有任务栏，只有一个命令行窗口。这种模式的效率更高，安全性更好。下面介绍如何在这种模式下配置打印服务器。

10.7.1　在 Windows Server Core 上安装打印服务器角色

① 在装有 Windows Server Core 的 ProfileServer 上，以域管理员身份登录。

② 如图 10-61 所示，输入 oclist，可以看到服务器已经安装和没有安装的服务器角色。

③ 如图 10-62 所示，输入 start /w ocsetup Printing-ServerCore-Role，在出现的提示框中单击“是”按钮，重启系统。



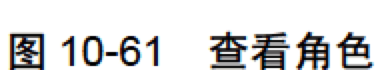


图 10-61　查看角色

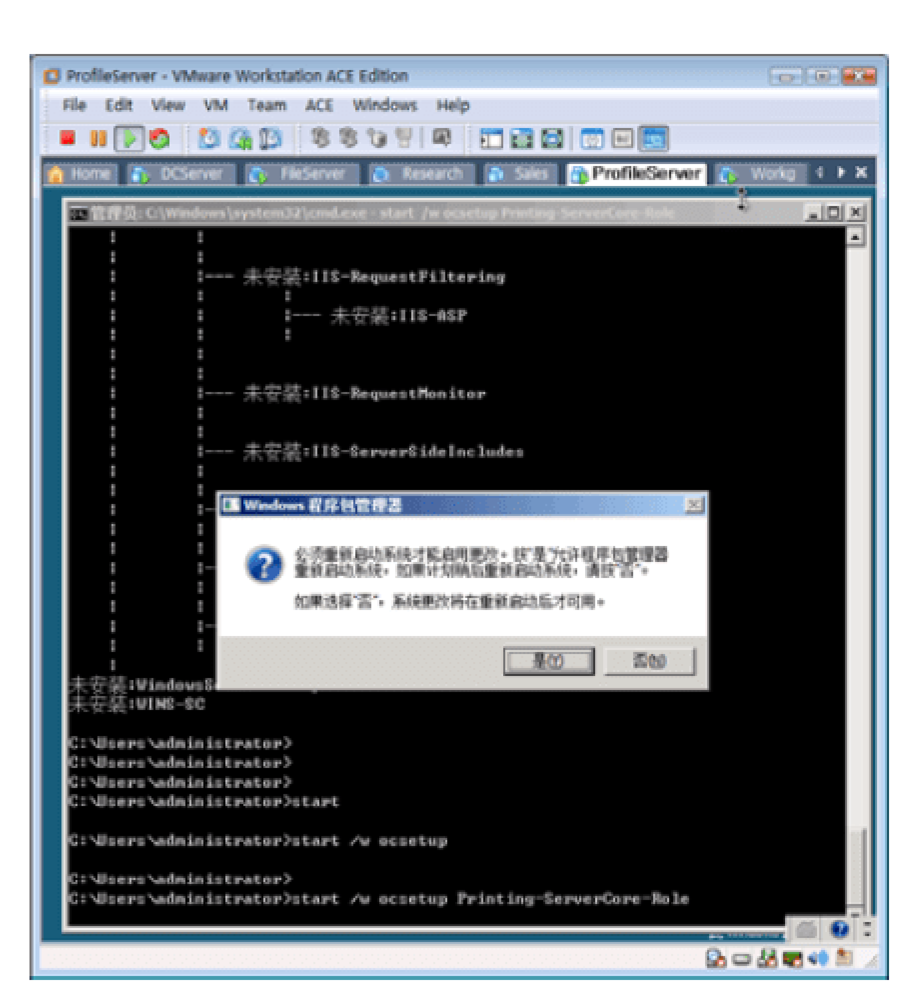


图 10-62　安装打印服务器角色

④ 如图 10-63 所示，输入 netsh firewall add portopening tcp 445 PrinterPort，打开防火墙 TCP 的 445 的端口。



注意：打开防火墙 445 端口，可以允许在 FileServer 计算机使用打印管理工具管理 Server Core 的打印服务。

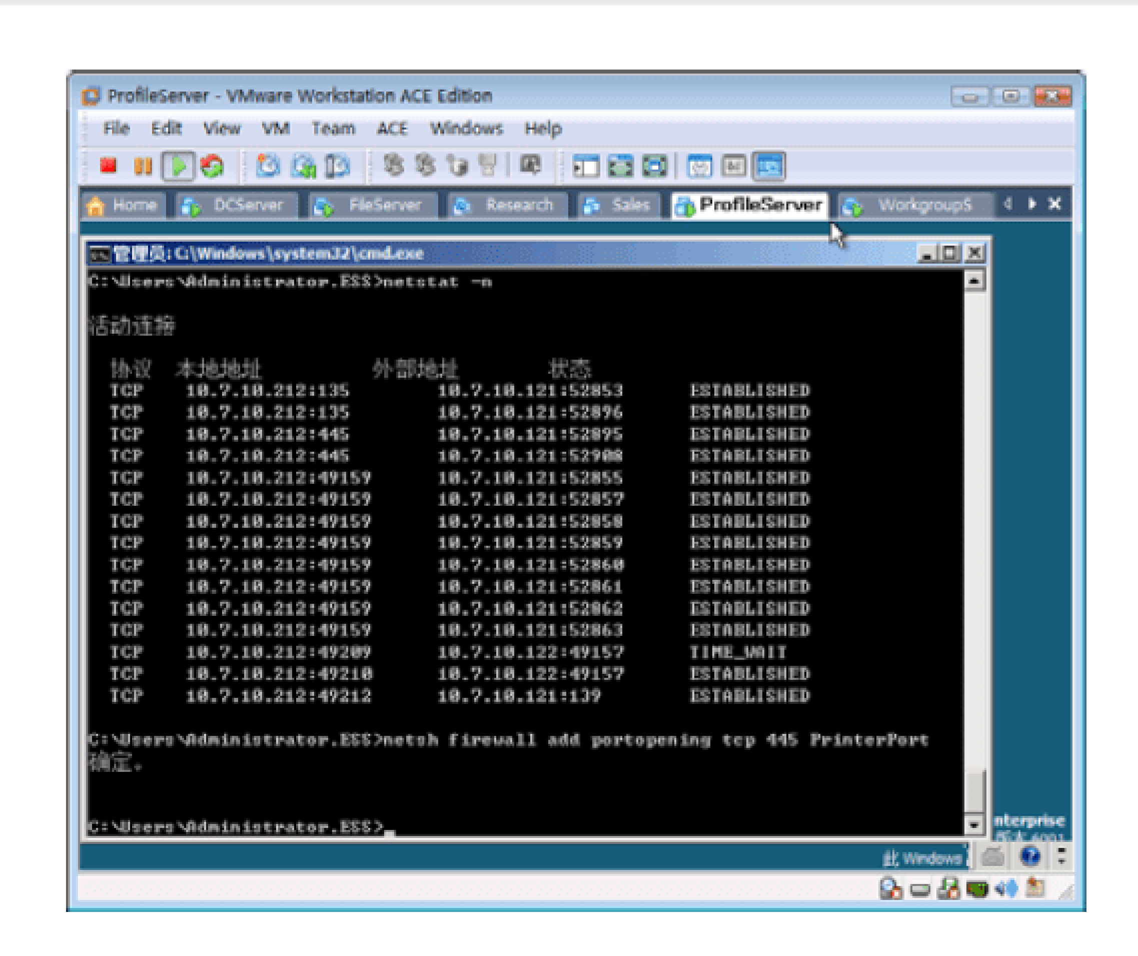


图 10-63　打开防火墙端口

10.7.2　在 Windows Server Core 上添加打印机驱动

将 HP 的打印设备连接到物理计算机。

① 如图 10-64 所示，选择 VM→Removable Devices→USB Devices→Hewlett-Packard Printer(Port2) 命令，这样由 ProfileServe 虚拟接通 USB 接口的打印机。

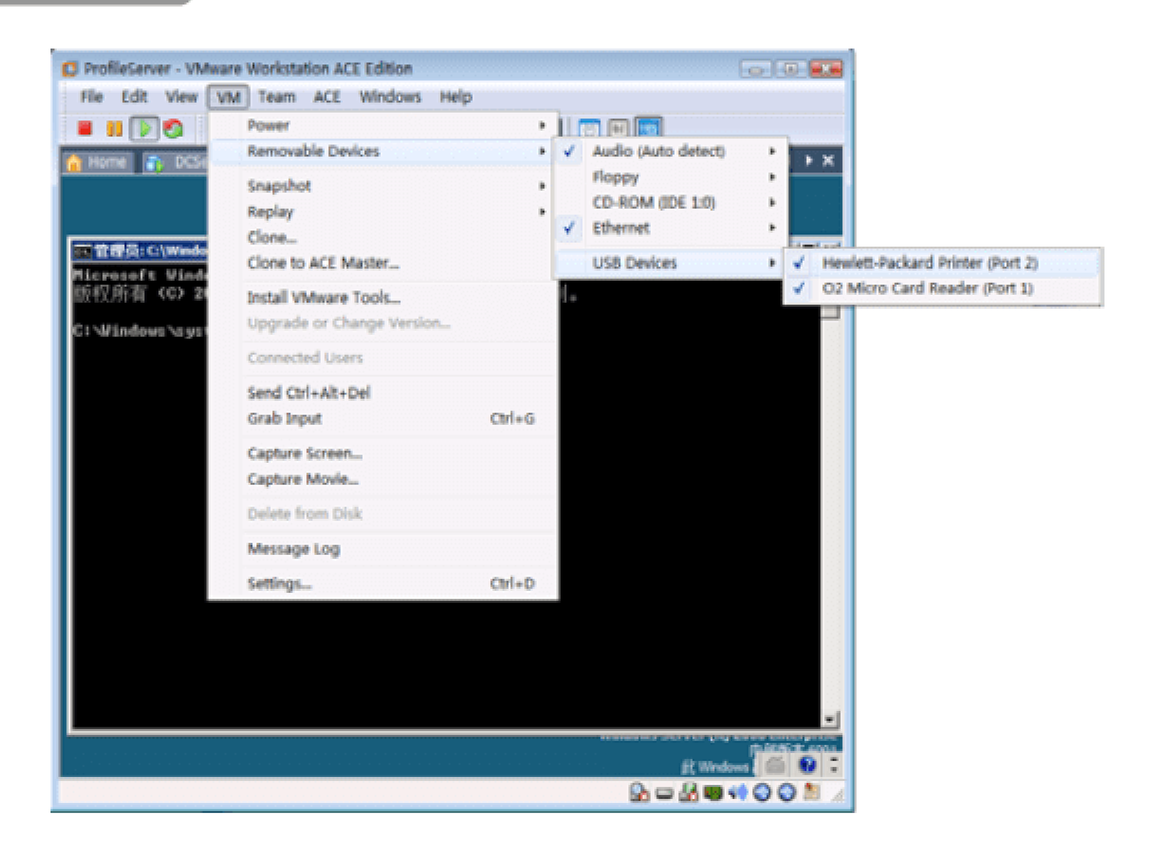


图 10-64　虚拟机 USB 接口

② 如图 10-65 所示，提示发现新硬件，单击“查找并安装驱动程序软件(推荐)”按钮。

③ 如图 10-66 所示，单击“不联机搜索”按钮。

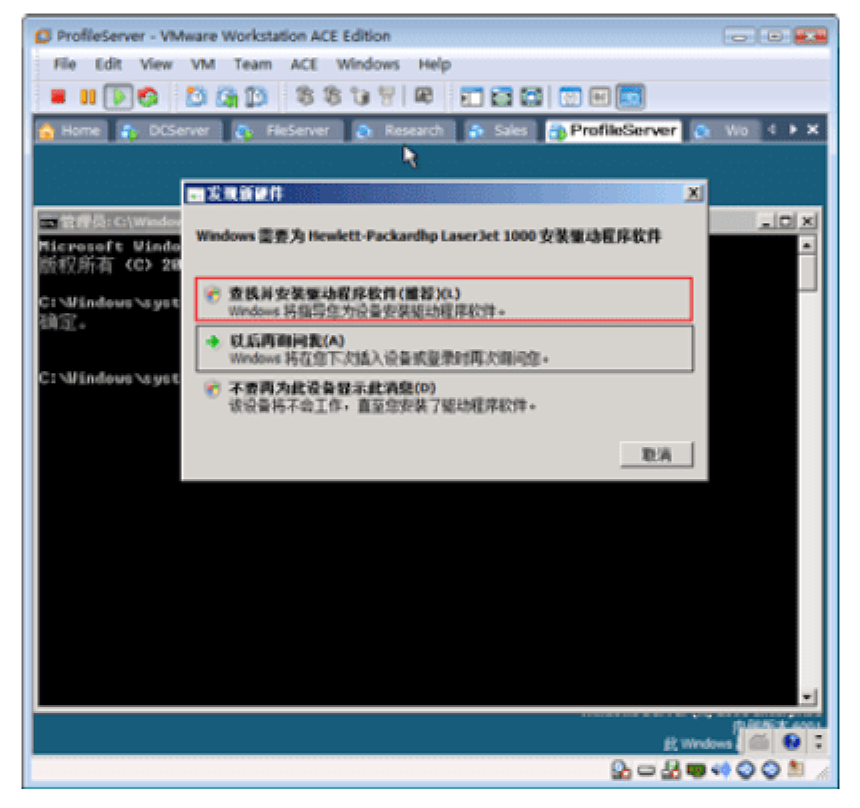


图 10-65　发现新硬件

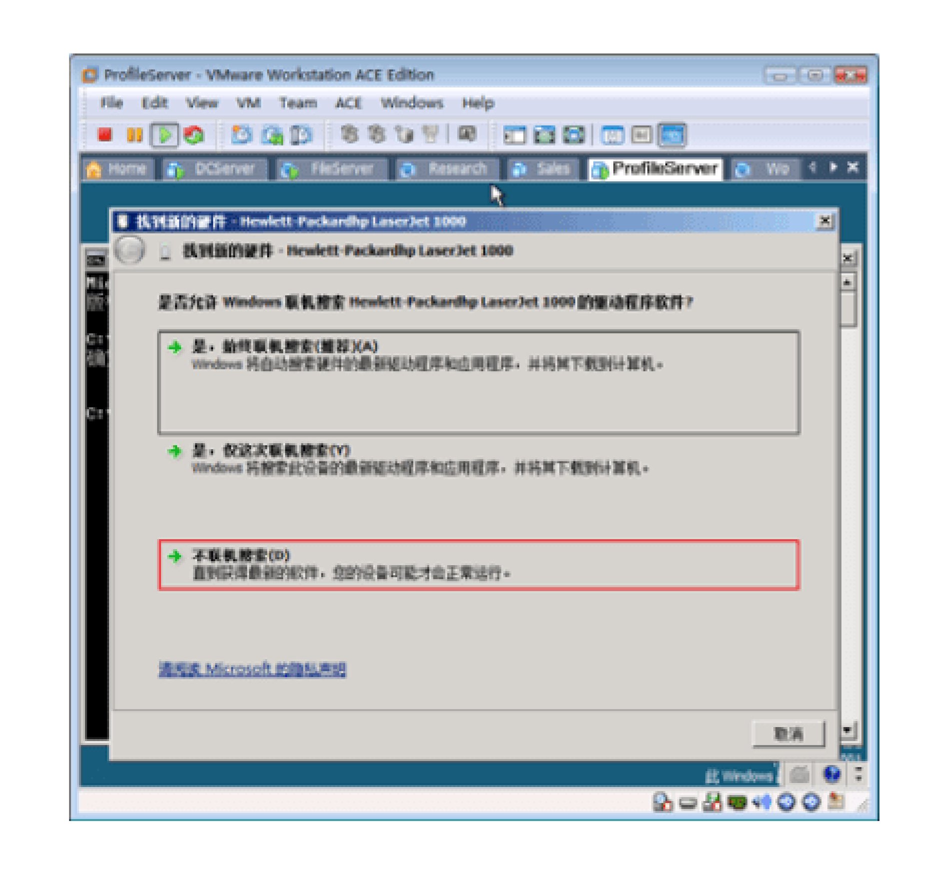


图 10-66　不联机搜索

④ 如图 10-67 所示，单击“我没有光盘，请显示其他选项”按钮。

⑤ 如图 10-68 所示，单击“浏览计算机以查找驱动程序软件(高级)”按钮。

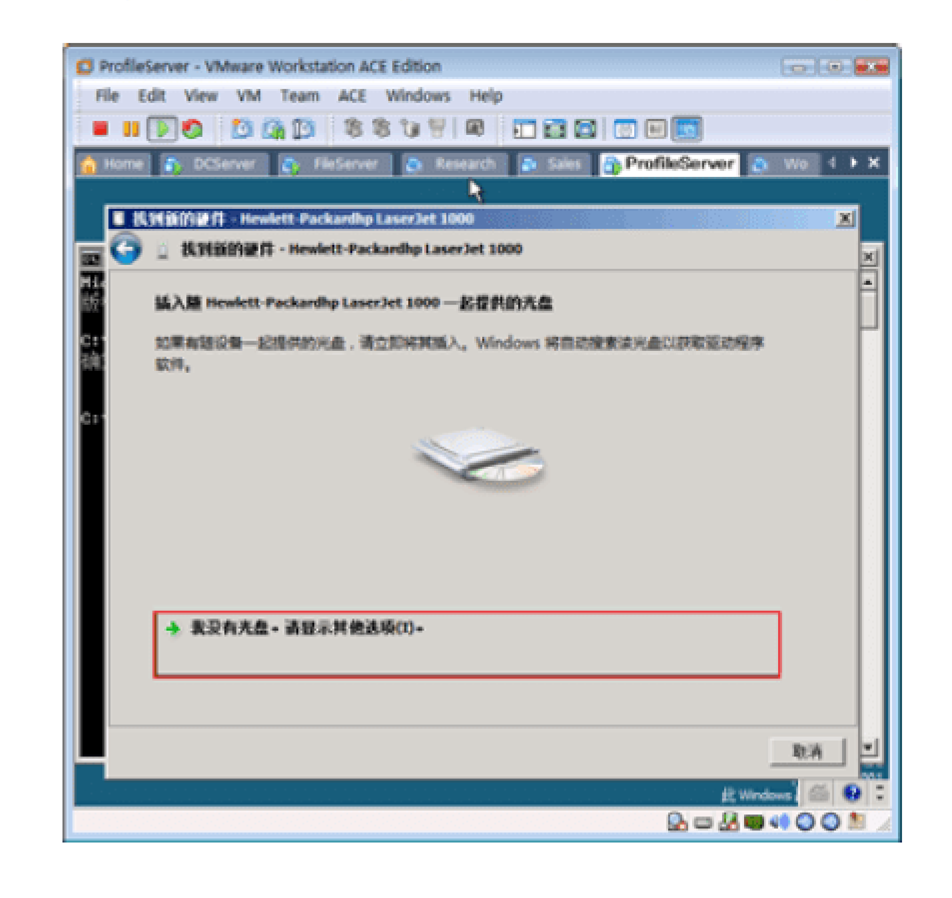


图 10-67　查找驱动

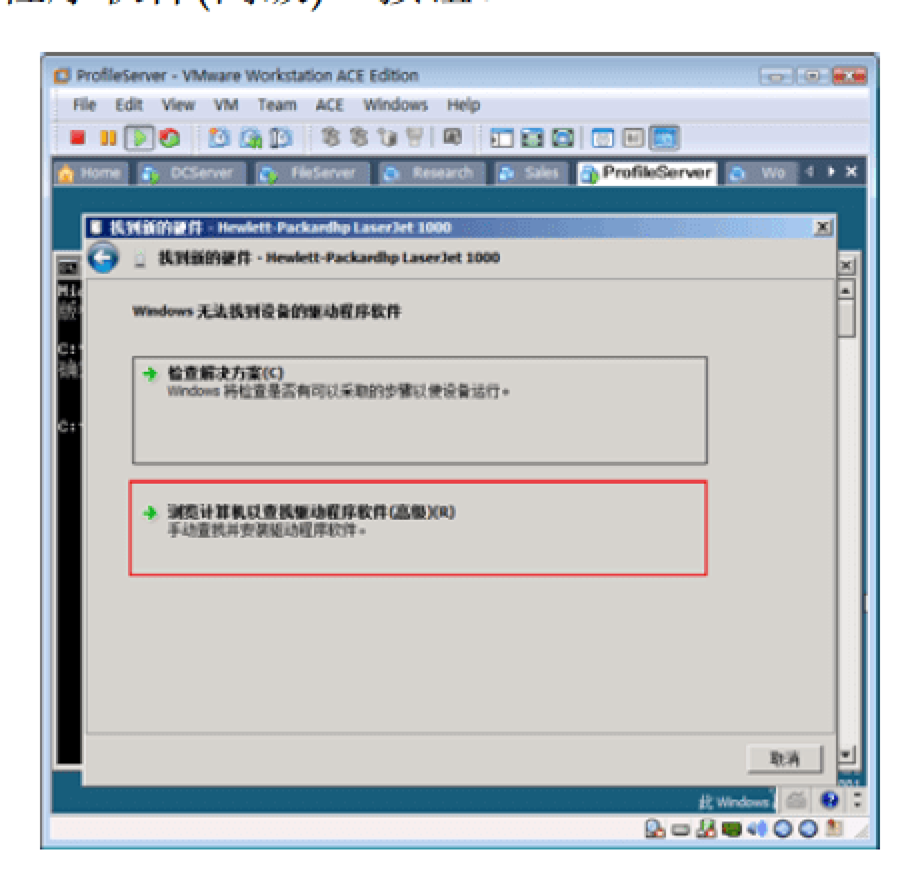


图 10-68　查找驱动(高级)

⑥　如图 10-69 所示，输入驱动程序位置，单击“下一步”按钮。

⑦　如图 10-70 所示，提示安装成功。

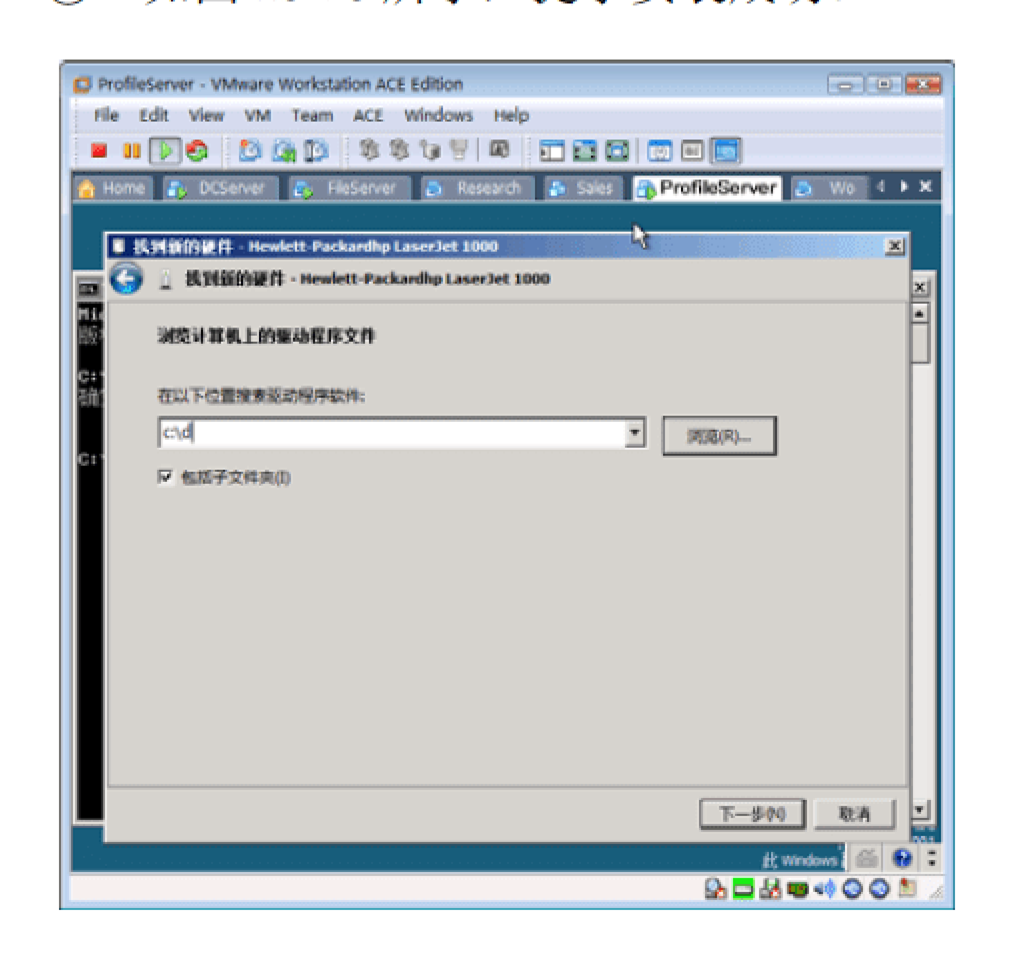


图 10-69　浏览驱动位置

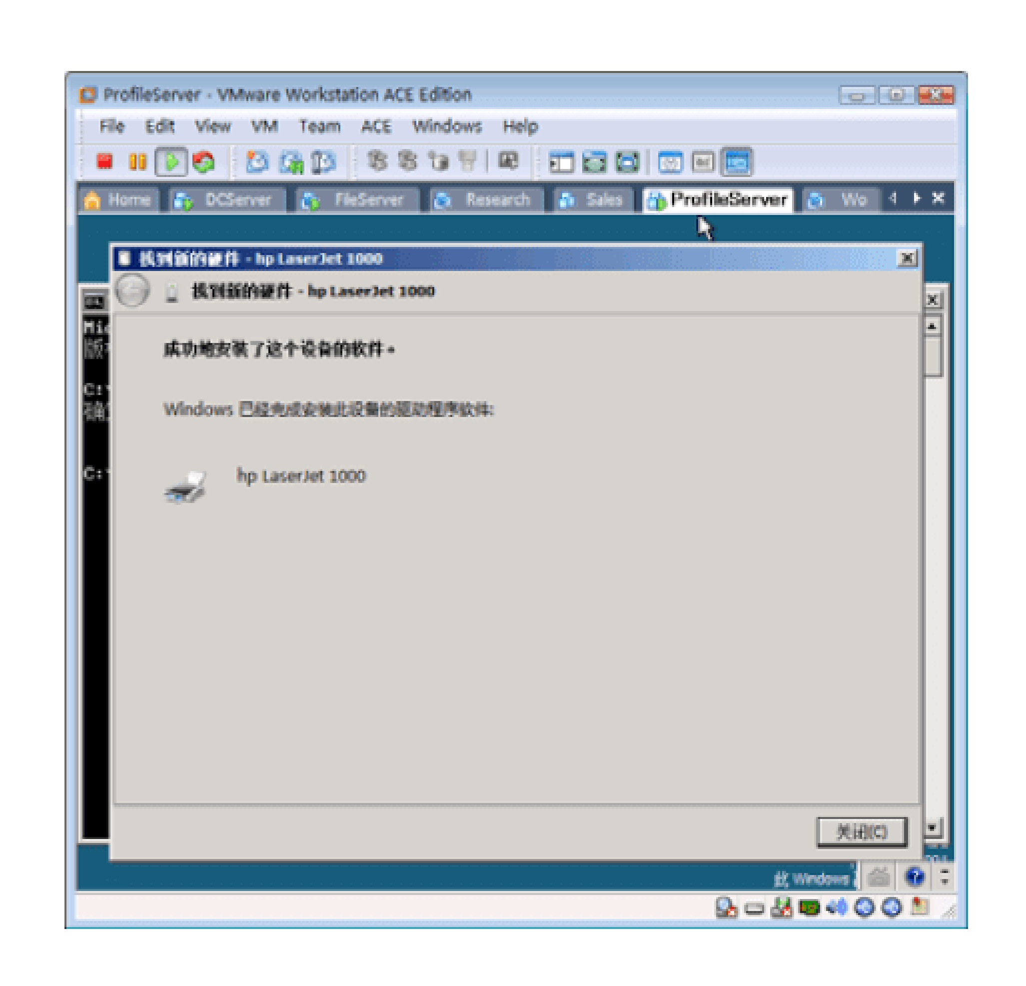


图 10-70　安装成功

10.7.3　使用图形化管理工具管理打印机

使用命令行管理 Windows Server Core 上的打印机很不方便，可以使用图形的管理工具管理 Windows Server Core 上的打印机。

①　在 FileServer 上，选择“开始”→“程序”→“管理工具”→“打印管理”命令。

②　如图 10-71 所示，右击打印服务器，在弹出的快捷菜单中选择“添加/删除服务器”命令。

③　如图 10-72 所示，在出现的“添加/删除服务器”对话框中，输入 profileserver，单击“添加到列表”按钮，然后单击“确定”按钮。

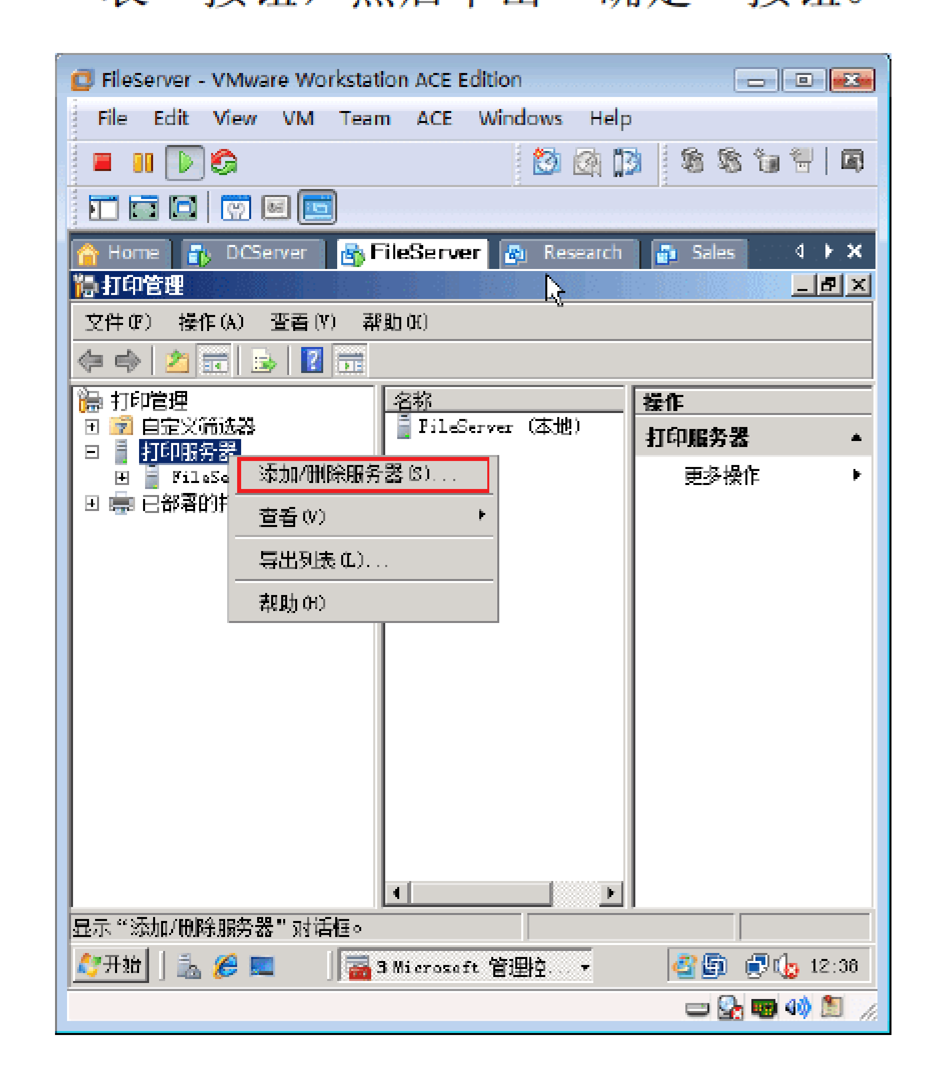


图 10-71　添加服务器

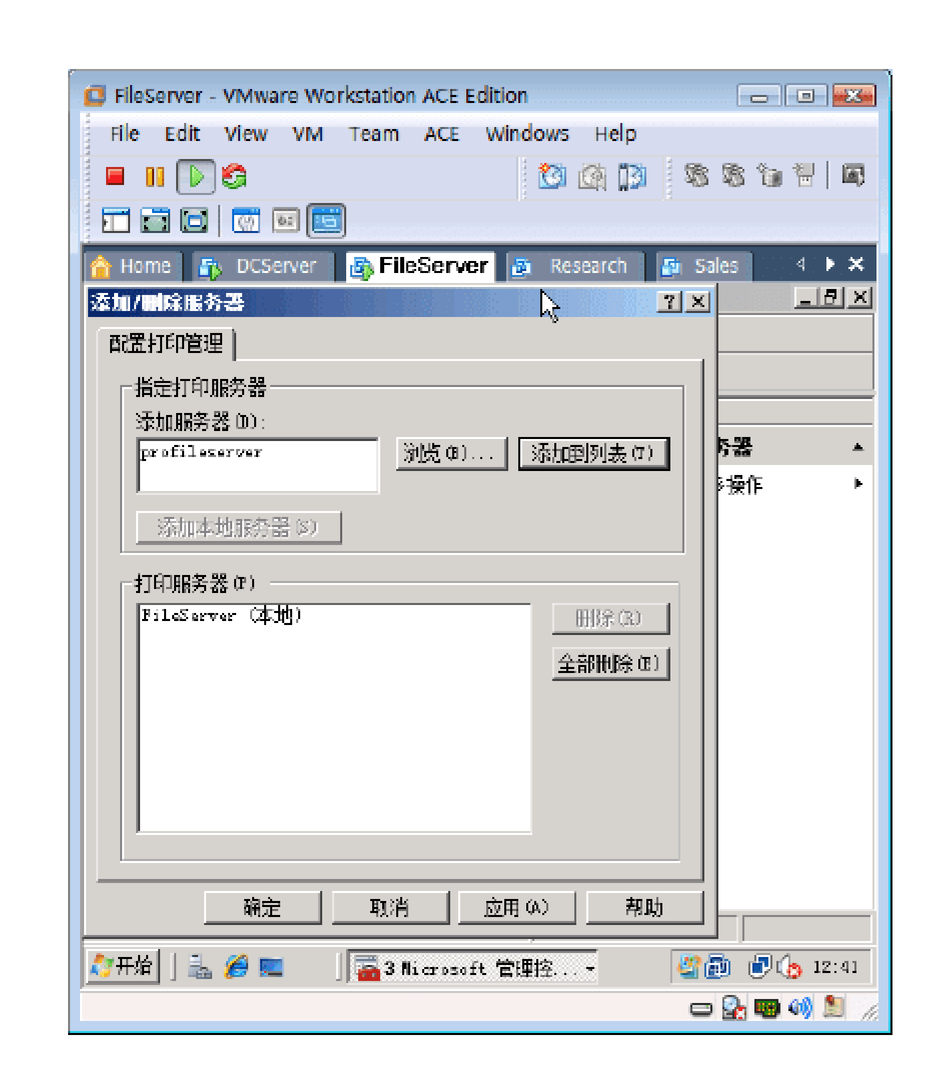


图 10-72　输入打印服务器名称

④ 如图 10-73 所示，右击 profileserver 下的打印机，在弹出的快捷菜单中选择“属性”命令。

⑤ 如图 10-74 所示，在出现的安装驱动对话框中，单击“是”按钮。

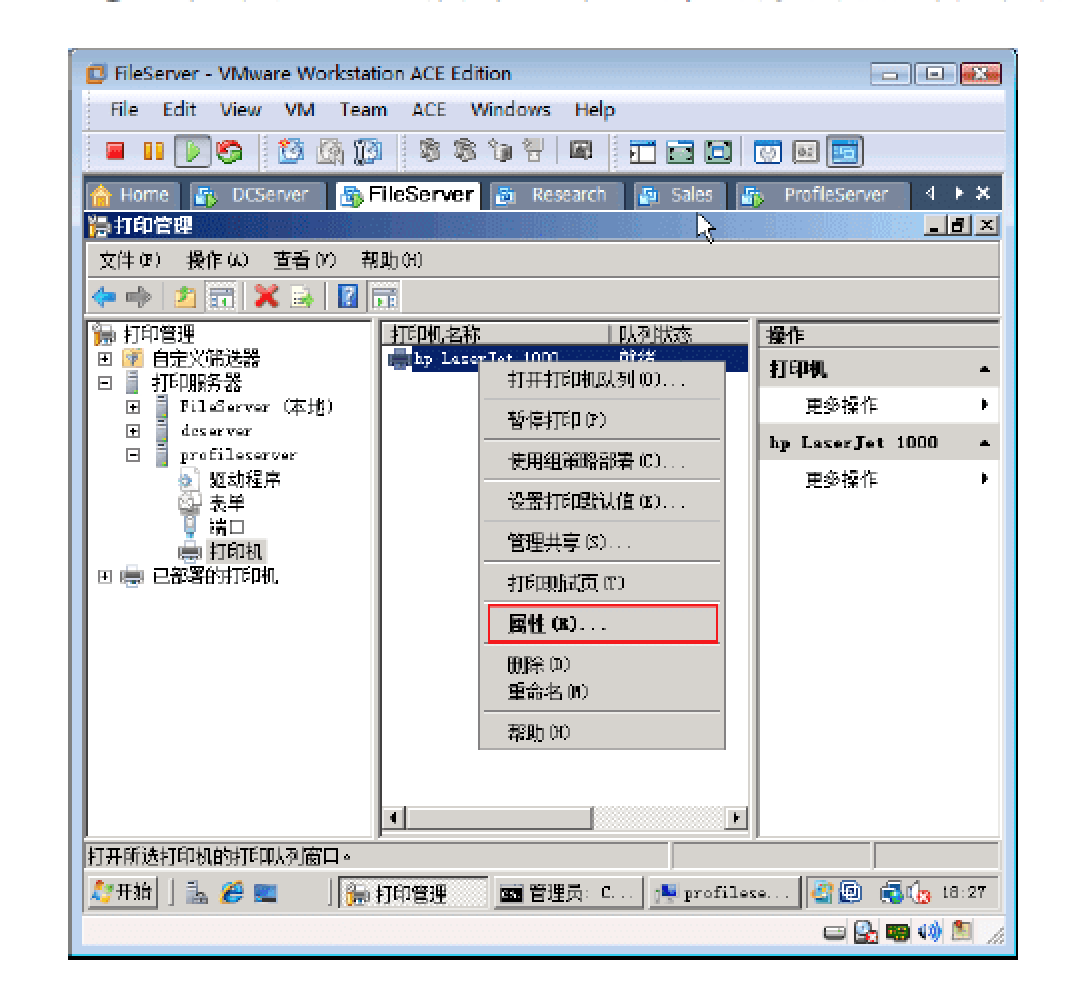


图 10-73 配置服务器属性

图 10-74 安装驱动

⑥ 如图 10-75 所示，选中 hp LaserJet 1000 型号打印机，单击“下一步”按钮。

⑦ 如图 10-76 所示，在出现的打印机属性对话框的“共享”选项卡中，选中“共享这台打印机”复选框，输入共享名。

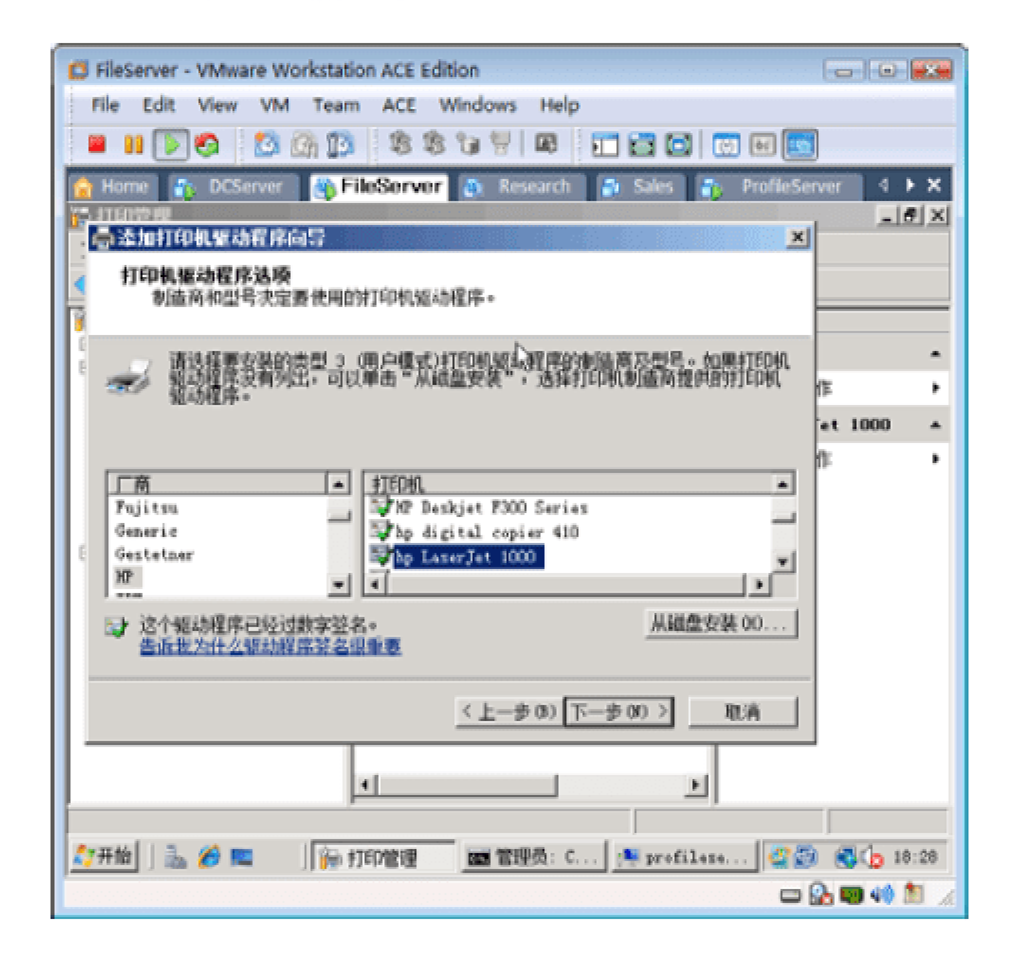


图 10-75 选择打印机型号

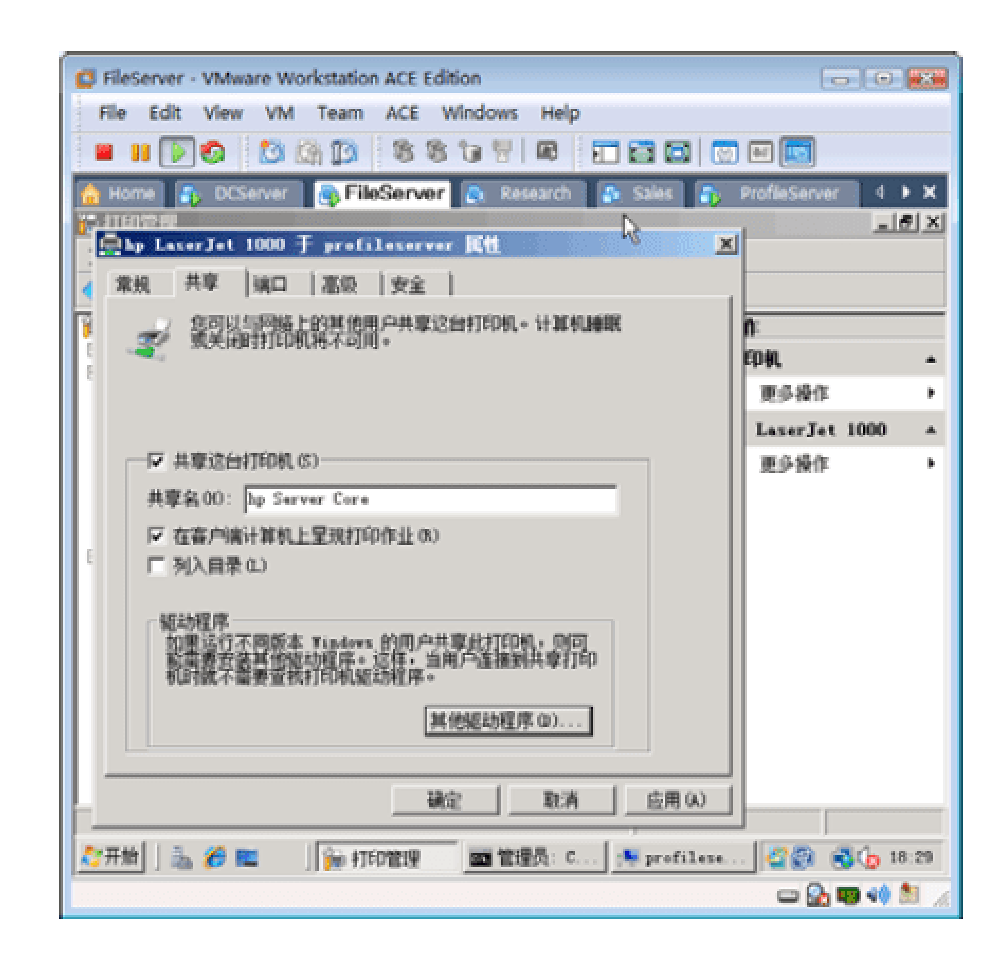


图 10-76 共享打印机

注意：使用打印管理可以管理其他打印服务器上的打印机属性，比如安全性设置、端口设置、列在目录中等。

⑧ 如图 10-77 所示，选择“开始”→“运行”命令，在出现的“运行”对话框中输入“\\profileserver”。可以看到 ProfileServer 共享的打印机。

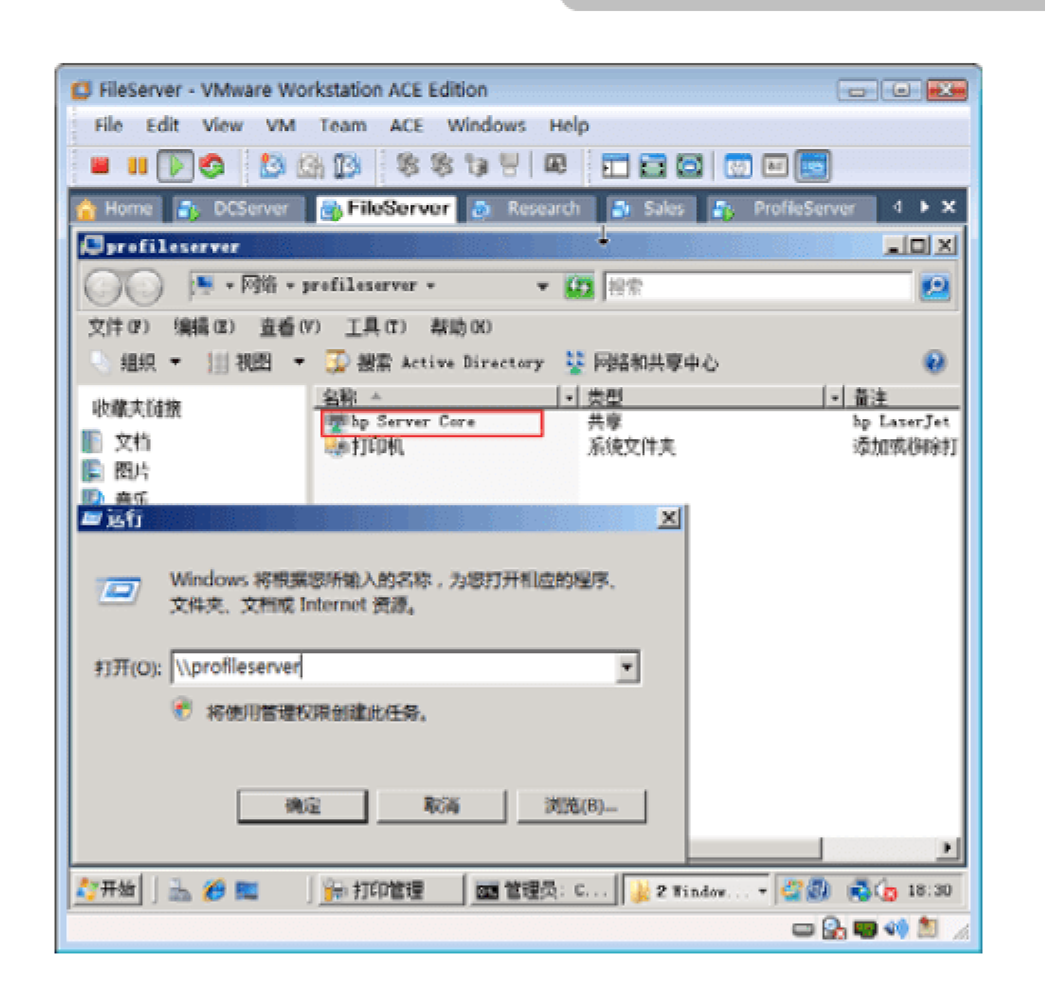


图 10-77　访问 Windows Server Core 共享的打印机

10.7.4　删除打印机

可以使用图形界面管理工具删除 Windows Server Core 打印服务器的打印机。

① 如图 10-78 所示，右击打印机，从弹出的快捷菜单中选择“删除”命令。

② 如图 10-79 所示，单击驱动程序，发现驱动程序还是保留在 Windows Server Core 打印服务器上了。

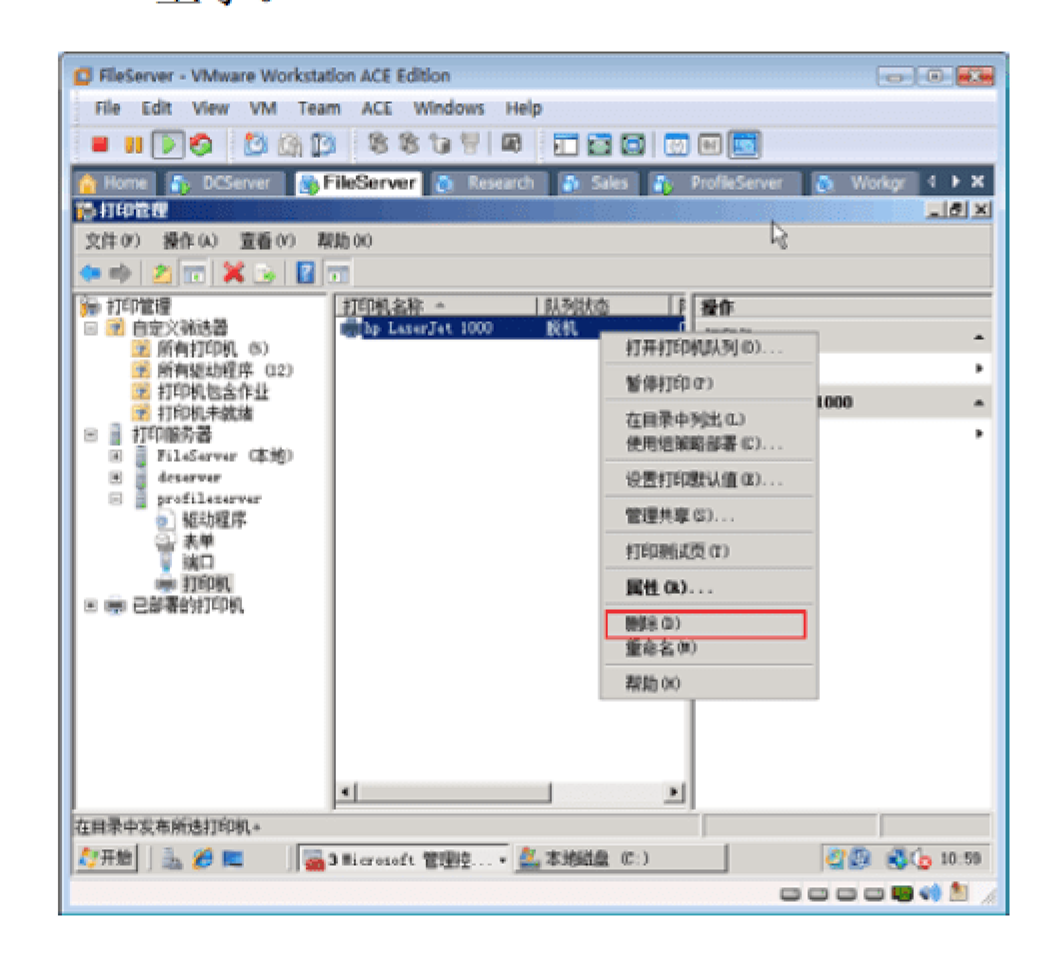


图 10-78　删除打印机

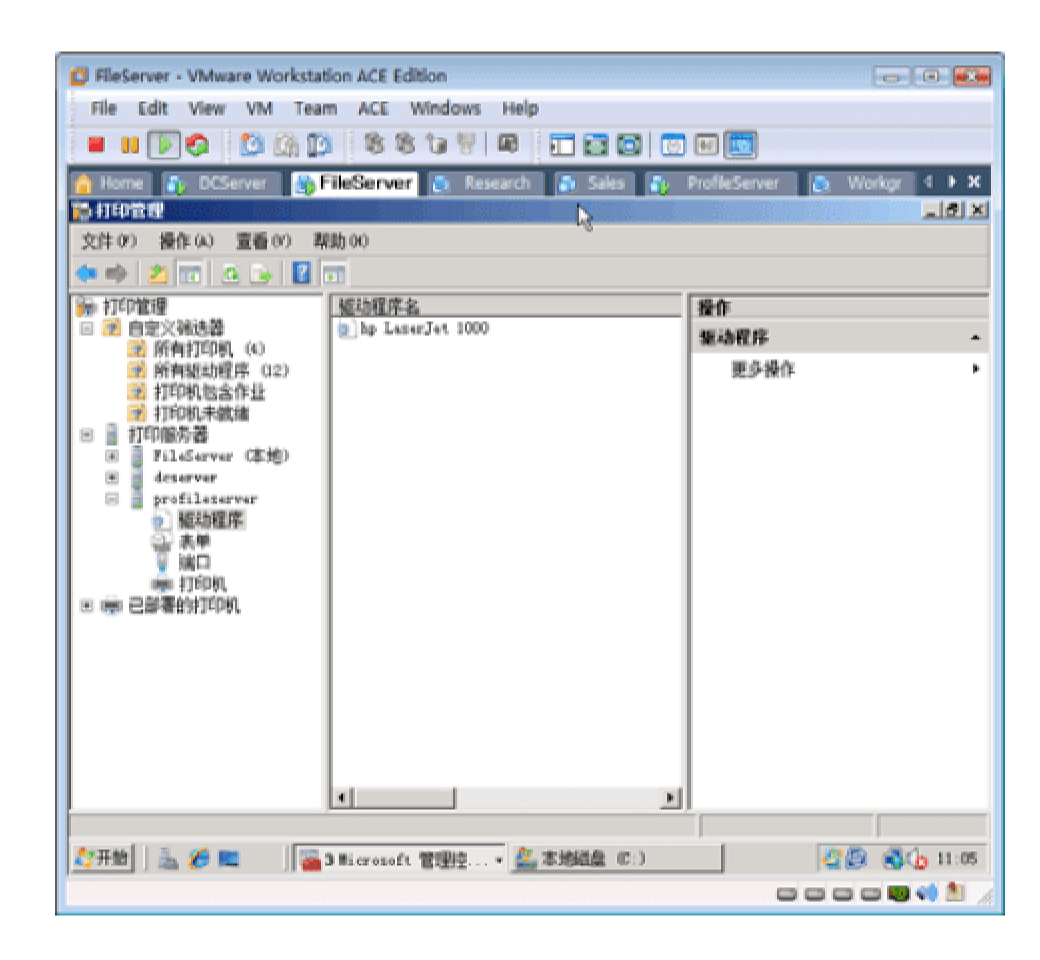


图 10-79　驱动没有删除

10.7.5　添加打印机

如果 Windows Server Core 已经有打印机驱动了，可以使用图形界面管理工具为 Windows Server Core 的打印服务器添加打印机。

在 Windows Server Core 打印机上必须连接好打印设备。

① 如图 10-80 所示，右击打印机，在弹出的快捷菜单中选择“添加打印机”命令。

② 如图 10-81 所示，在出现的对话框中，选中“使用现有的端口添加打印机”单选按钮，选定 USB 虚拟端口，单击“下一步”按钮。

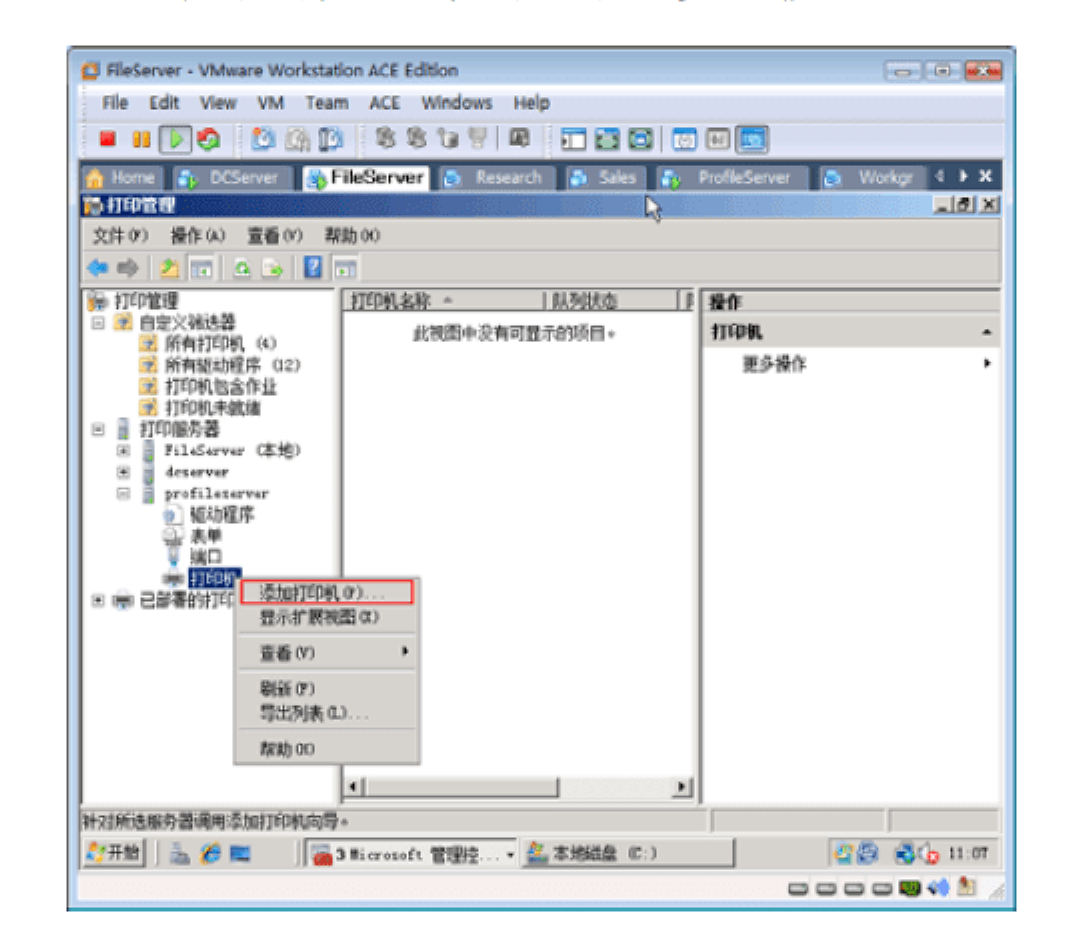


图 10-80 添加打印机

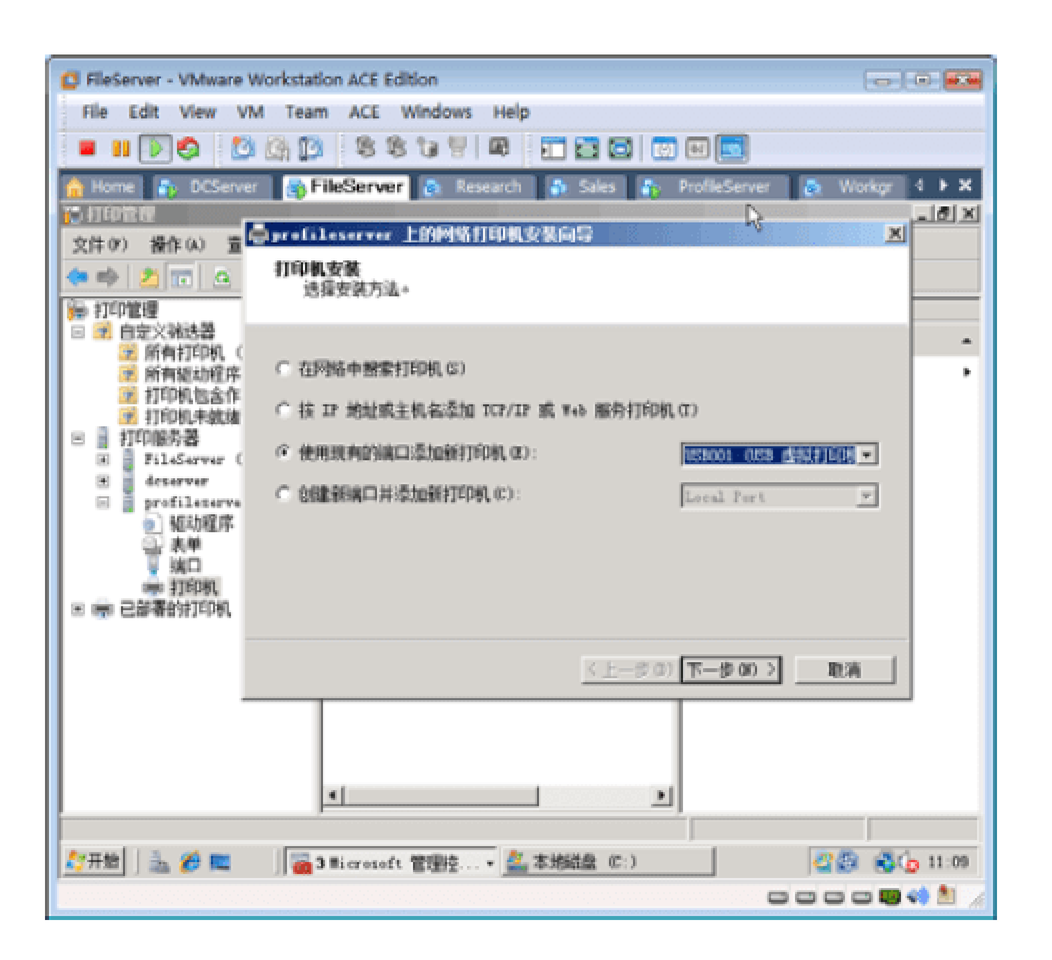


图 10-81 选择端口

③ 如图 10-82 所示，选中“使用计算机上现有的打印机驱动程序”单选按钮，单击“下一步”按钮。

④ 如图 10-83 所示，输入共享名和打印机名，单击“下一步”按钮。

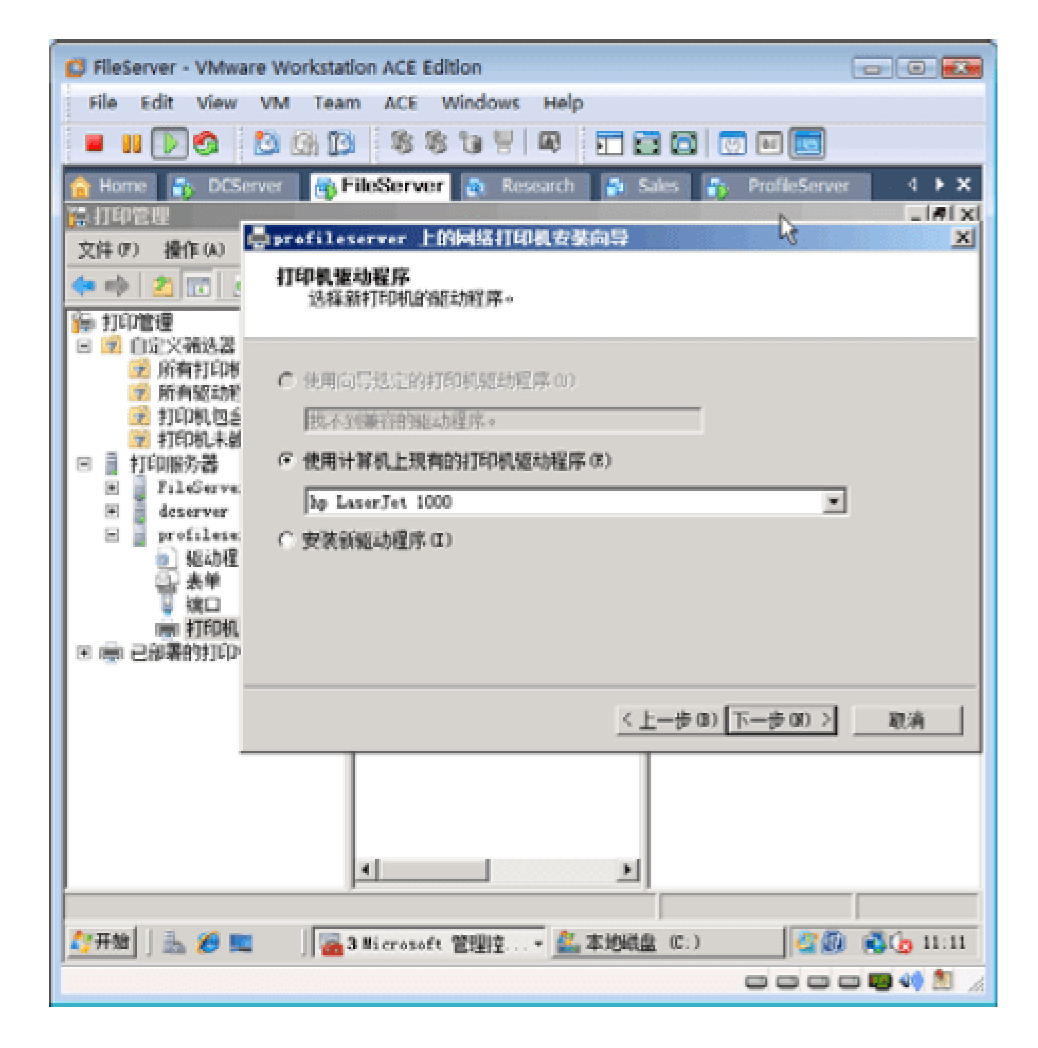


图 10-82 使用现有驱动

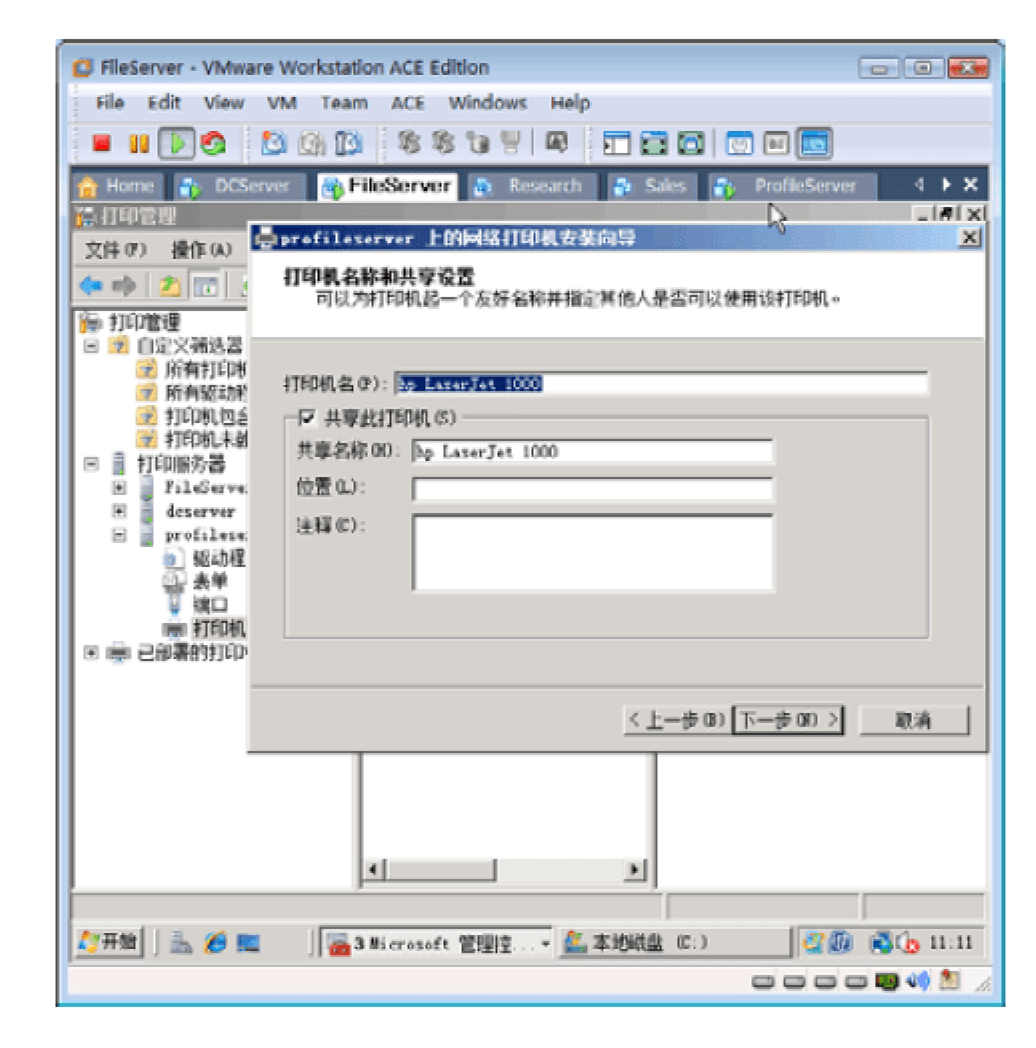


图 10-83 输入打印机名称



注意：如果打印设备没有连接好，会提示出现一个错误，但是打印机驱动已经添加成功。

第 11 章　磁 盘 管 理

无论文件服务器、FTP 服务器还是数据库服务器，都需要磁盘能够有好的性能来快速响应大量并发用户的请求，这就要求磁盘有很好的 I/O 吞吐量。

重要的文件服务器还需要有磁盘冗余，以避免磁盘的硬件故障造成数据丢失或不可访问。

在 Windows Server 2000、Windows Server 2003 以及 Windows Server 2008 中均提供了软 RAID 的功能，可以在没有 RAID 卡的服务器上通过创建软 RAID 实现较好的读取和写入功能，以及容错功能。

在动态磁盘可以创建带区卷、镜像卷以及 RAID-5 卷。其中 RAID-0 和 RAID-5 有容错能力，RAID-0 有很好的读写性能。

关键词

- 初始化磁盘
- 实现磁盘分区
- 查看和更新磁盘属性
- 更改驱动器号和路径
- 实现磁盘的转换
- 管理动态卷
- 动态磁盘灾难恢复
- 远程管理 Windows Server Core 的磁盘
- 动态磁盘迁移

本章将重点介绍如何实现磁盘管理，具体内容包括：磁盘管理的基本概念、磁盘管理项目，如何管理驱动器号和路径，如何实现磁盘的转换，如何创建带区卷、镜像卷、RAID-5 和跨区卷及如何修复失败的镜像卷和 RAID-5，远程管理 Windows Server Core 的磁盘，将动态磁盘迁移到其他服务器上。

11.1 本章环境

本章学习环境如图 11-1 所示。

- DCServer 是 Ess.com 域中的域控制器，安装 Windows Server 2008 企业版操作系统。
- FileServer 是 Ess.com 域中的文件服务器，有 4 块硬盘，安装 Windows Server 2008 企业版操作系统。
- Research 是 Ess.com 域中的备用文件服务器，安装 Windows Server 2008 企业版操作系统。
- ProfileServer 是 Ess.com 域中的文件服务器，有 4 块硬盘，安装 Windows Server Core 系统。

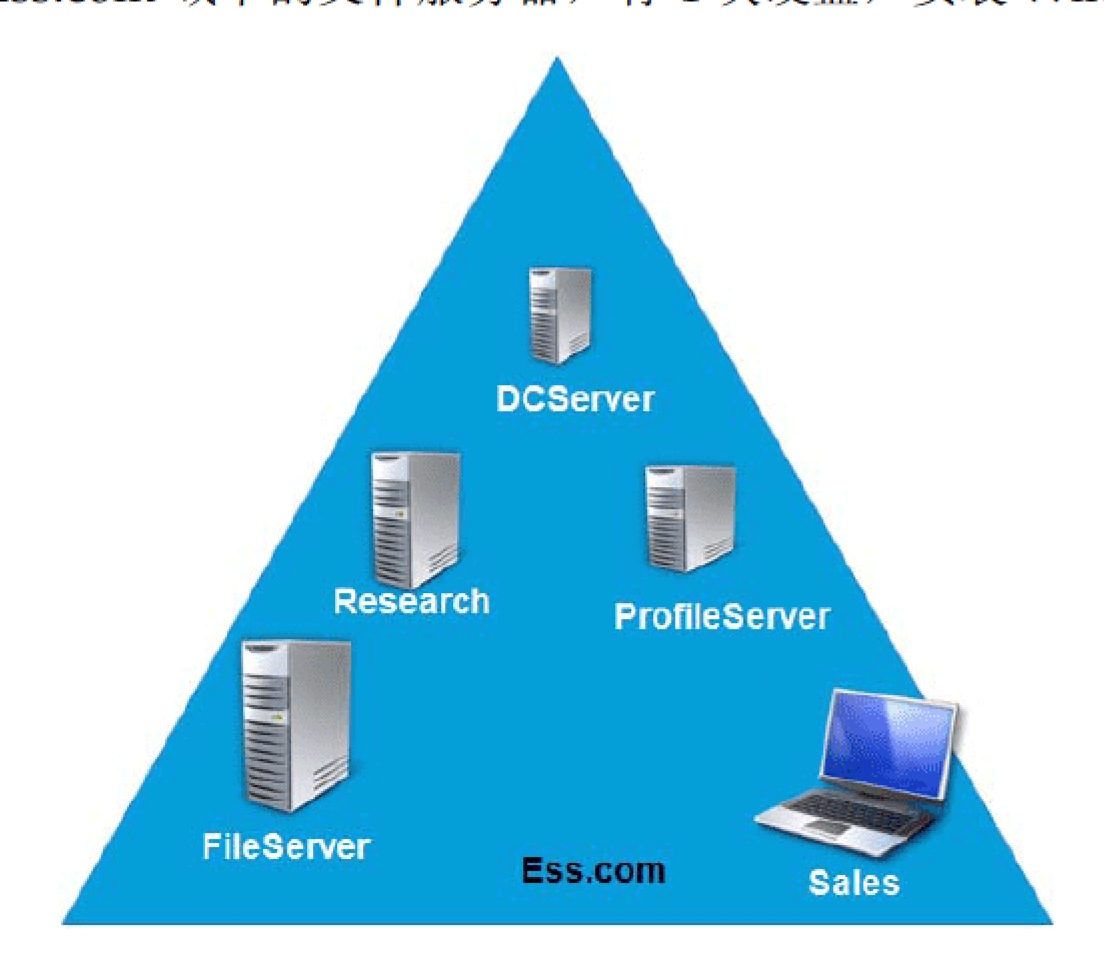


图 11-1 本章实战环境

11.2 磁盘管理

可以使用 Windows XP Professional 和 Windows Server 2008 家族操作系统中的 Disk Management 来执行与磁盘相关的任务，如创建和格式化分区和卷、分配驱动器号。当我们在计算机中安装一块新磁盘时，Windows Server 2008 将这块磁盘作为一块基本磁盘来进行配置。基本磁盘在 Windows Server 2008 中是默认的存储介质。

磁盘管理程序是用于管理硬盘、卷或它们所包含的分区的系统实用工具。利用磁盘管理，可以初始化磁盘、创建卷，使用 FAT、FAT32 或 NTFS 文件系统格式化卷以及创建容错磁盘系统。磁盘管理可以在不需要重新启动系统或中断用户的情况下执行多数与磁盘相关的任务；大多数配置更改将立即生效。

在 Windows Server 2008 中的 Disk Management 具有以下几个新特点。

- 基本和动态磁盘存储。基本磁盘包含有基本卷，例如主磁盘分区和扩展分区中的逻辑驱动器。动态磁盘包含所提供的功能比基本磁盘要多的动态卷，如在 Windows 2000 Server 家族或

Windows Server 2008 家族操作系统上创建容错卷。

- 本地和远程磁盘管理。使用 Disk Management 可以管理运行 Windows 2000、Vista 或 Windows Server 2008 家族操作系统的任何远程计算机。
- 装入的驱动器。使用 Disk Management 可以在本地 NTFS 卷上的任何空文件夹中连接或装入本地驱动器。装入的驱动器使数据更容易访问，并赋予用户基于工作环境和系统使用情况管理数据存储的灵活性。
- 支持 MBR 和 GPT 磁盘。Disk Management 在基于 x86 的计算机上提供对主启动记录 (MBR) 磁盘的支持，以及在基于 Itanium 的计算机中提供对 MBR 和 GUID 分区表 (GPT) 磁盘的支持。
- 支持存储区域网络 (SANs)。为了在 Windows Server 2008 Enterprise Edition 和 Windows Server 2008 Datacenter Edition 之间的存储区域网络有良好的互操作性，新磁盘上的卷加入系统时，不默认自动装入和分配驱动器符。

我们可以使用 Disk Management 来配置和管理计算机的存储空间以及执行所有的磁盘管理任务，也可以使用磁盘管理来转换磁盘的存储类型，创建和扩展卷以及其他的磁盘管理工作，例如：管理驱动器盘符和路径。

当我们创建了一个新的控制台，并添加了 Disk Management 单元后，就可以通过 Disk Management 控制台来管理本地和远程计算机上的磁盘。通过在控制台中添加多个 Disk Management 单元，可以在一个控制台中同时管理本地和多个远程计算机上的磁盘。作为管理员组(Administrators group)或服务器操作员组(Server Operators group)的成员，我们可以从网络中任何一台运行 Windows Server 2008 的计算机上管理域中或信任域中运行 Windows Server 2008 计算机上的磁盘。

11.2.1　初始化磁盘

磁盘分区是一种划分物理磁盘的方法，以便使每一部分都能够作为单独的单元运行。在基本磁盘上创建分区时，可将磁盘分成一个或多个区域，不同的分区通常具有不同的驱动器号(如 C：和 D：)。一个基本磁盘最多可以创建四个主磁盘分区，或者三个主磁盘分区和一个扩展分区。(扩展分区可以细分为逻辑驱动器，而主磁盘分区无法再细分)在我们创建了一个分区之后，必须对该分区按不同的文件系统(NTFS、FAT)进行格式化，然后才可以在该分区上存储数据。

利用分区，我们可以将系统文件和应用程序分别安装在不同的分区上。例如，一个管理员可以将系统文件安装在字母 C 标识的分区上，而将应用程序文件安装在字母 D 标识的分区上。

示例：实现磁盘分区。

给服务器添加 3 块 IDE 接口的硬盘。

① 关闭 FileServer，如图 11-2 所示，单击 Edit virtual machine settings，在出现的 Virtual Machine Settings 对话框中，选中 CD-ROM，单击 Remove 按钮。

> **注意：**因为 IDE 接口最多只能接四个硬盘，光驱占用一个，就不能添加三块 IDE 接口的硬盘了，因此需要删除 CD-ROM。

② 如图 11-3 所示，单击 Add，在出现的对话框中，选中 Hard Disk，单击 Next 按钮。

③ 如图 11-4 所示，在出现的选择磁盘对话框中，选中 Create a new virtual disk 单选按钮，单击 Next 按钮。

④ 如图 11-5 所示，在出现的选择磁盘类型对话框中选中 IDE 单选按钮，单击 Next 按钮。

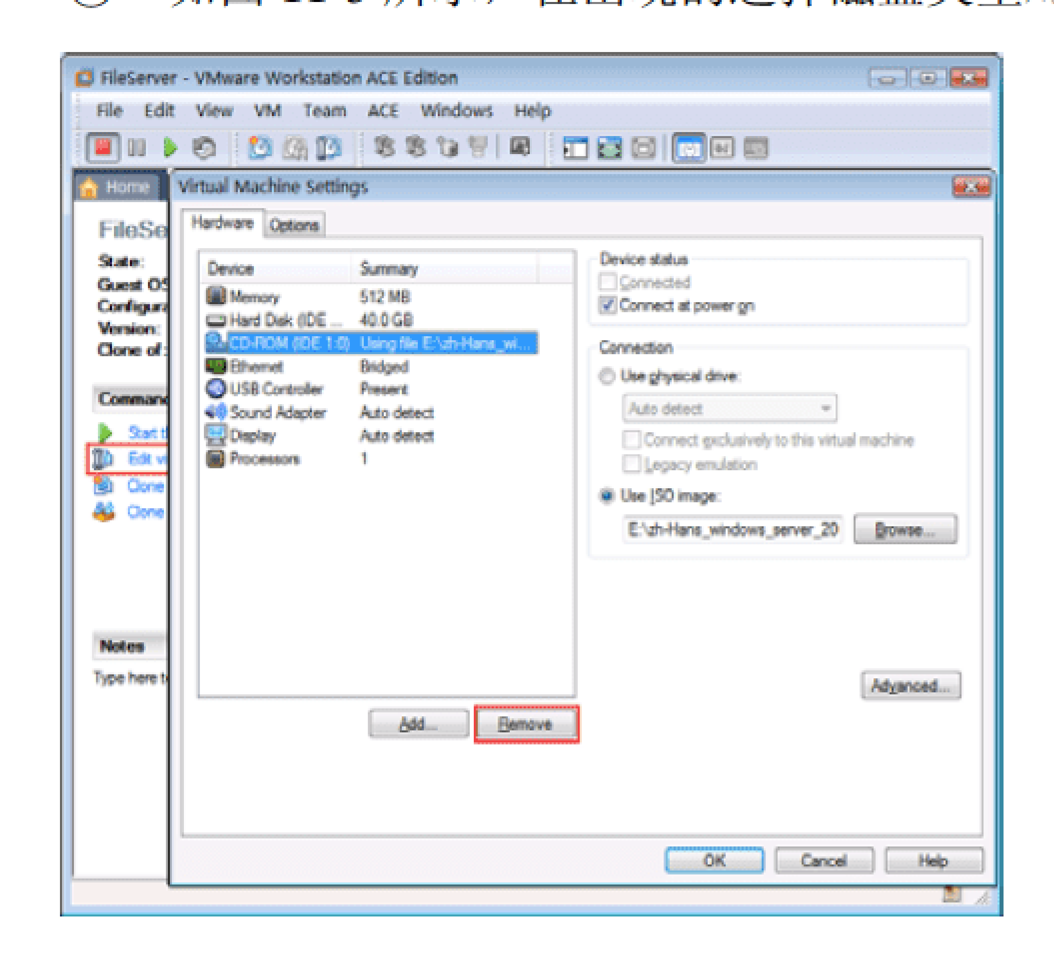


图 11-2　删除光驱

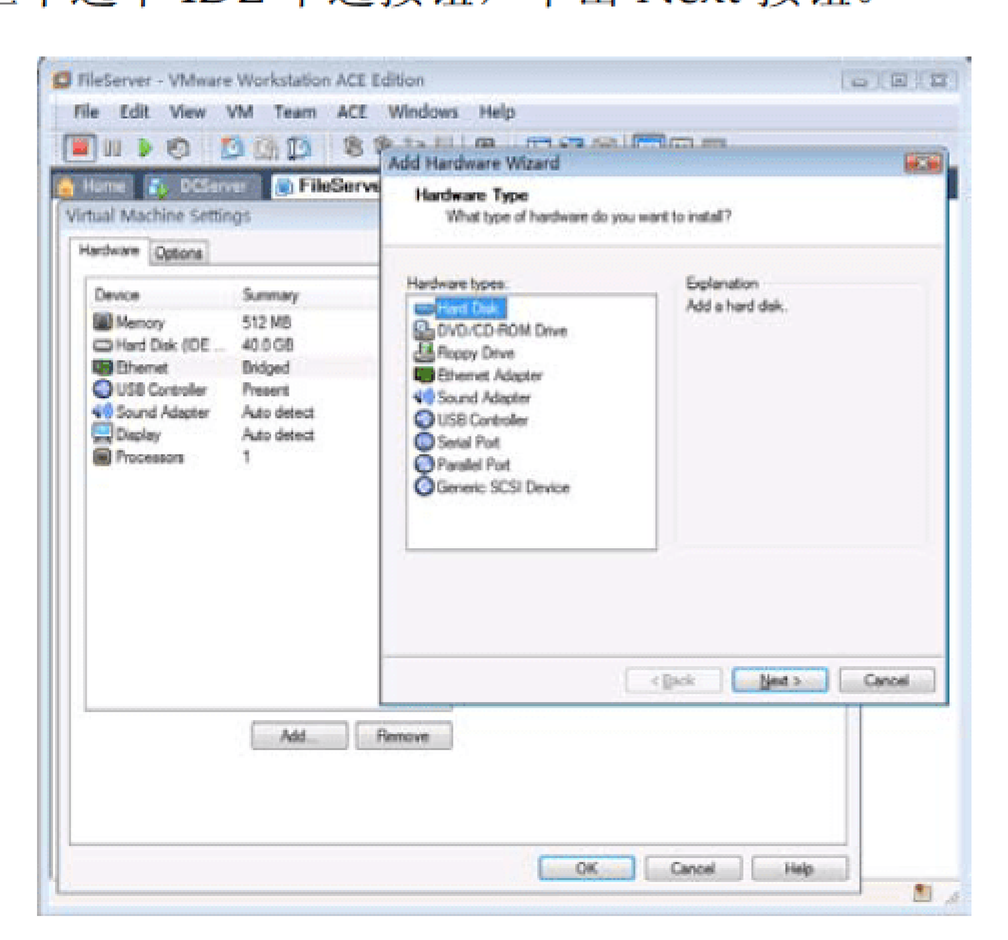


图 11-3　添加硬盘

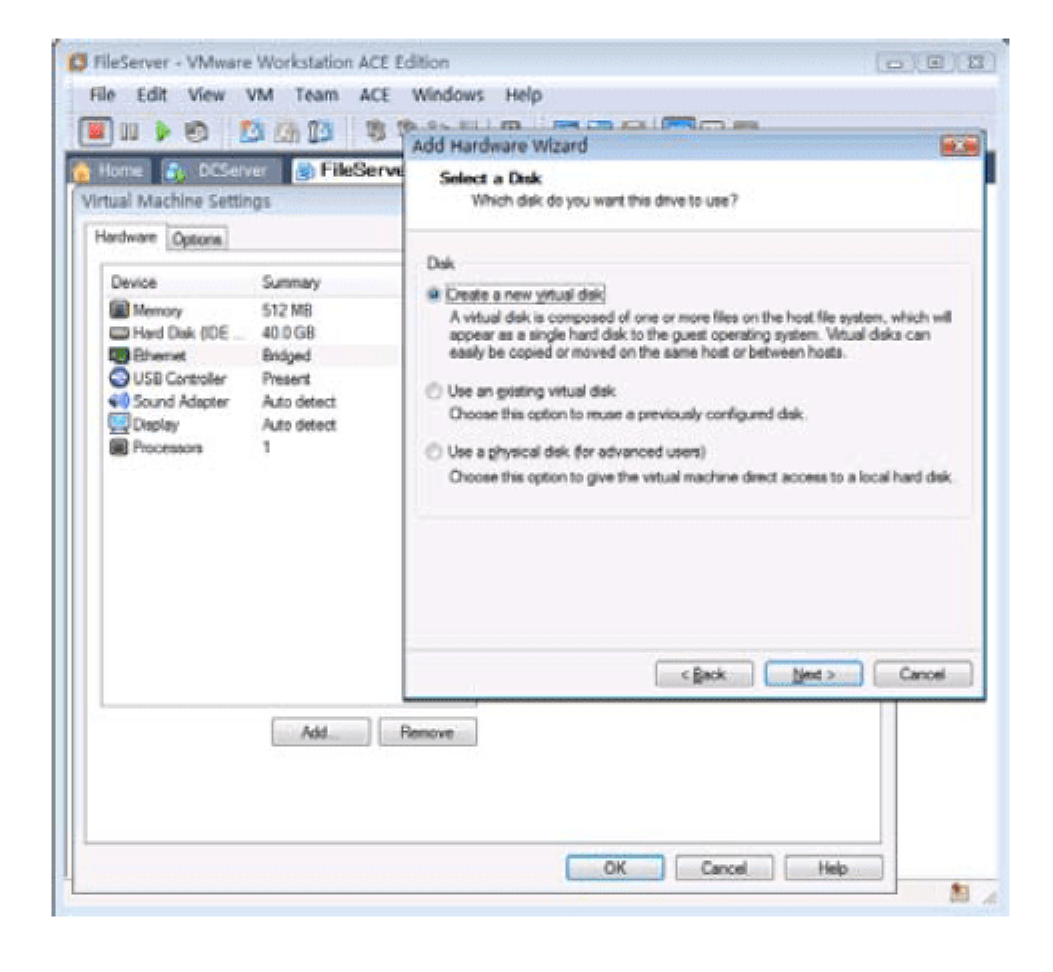


图 11-4　选择磁盘

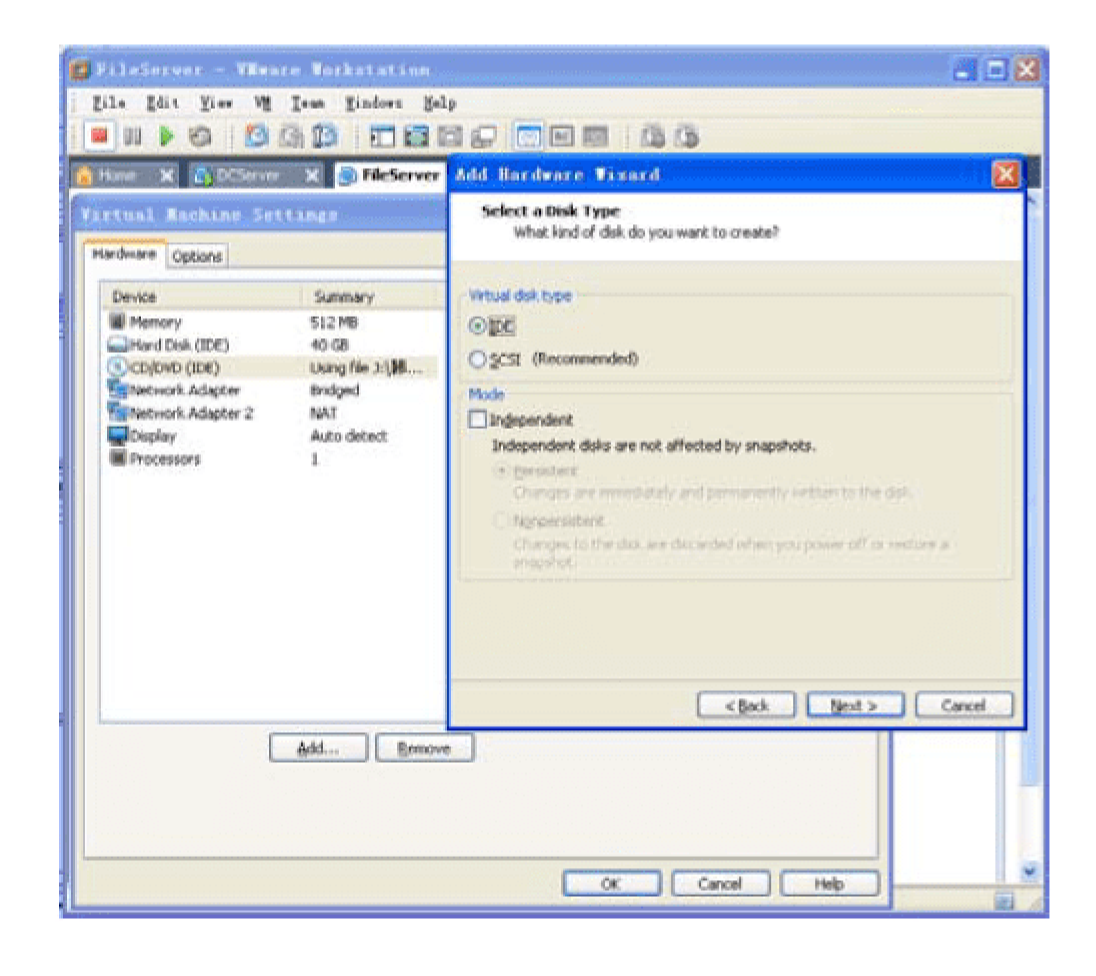


图 11-5　选择磁盘类型

⑤ 如图 11-6 所示，在出现的指定磁盘文件对话框，输入磁盘文件的名称 FirstDisk.vmdk，单击 Next 按钮。

⑥ 如图 11-7 所示，在出现的指定磁盘大小对话框中，输入磁盘大小 40 GB，单击 Finish 按钮，完成硬盘添加。

⑦ 使用相同的方法添加 SecondDisk.vmdk 和 Third.vmdk 两块 40 GB 硬盘。

⑧ 启动 FileServer。

⑨ 以管理员身份登录到 FileServer，打开服务器管理器。

⑩ 选择“存储”→“磁盘管理”命令，在出现的初始化磁盘对话框，选中“GPT(GUID 分区表)”，单击“确定”按钮。



提示： 在我们为某台计算机安装一块新硬盘时，必须先对该硬盘进行初始化，然后再对该硬盘进行分区操作。主启动记录（MBR）磁盘使用标准的 BIOS 分区表。GUID 分区表（GPT）磁盘使用可扩展固件接口（EFI）。MBR 磁盘不支持每个磁盘上多于四个分区。对于大于 2 TB 的磁盘，不建议使用 MBR 分区方式。只要磁盘是空的而且未包含任何卷，就可以将其从 GPT 分区形式更改为 MBR 分区形式。

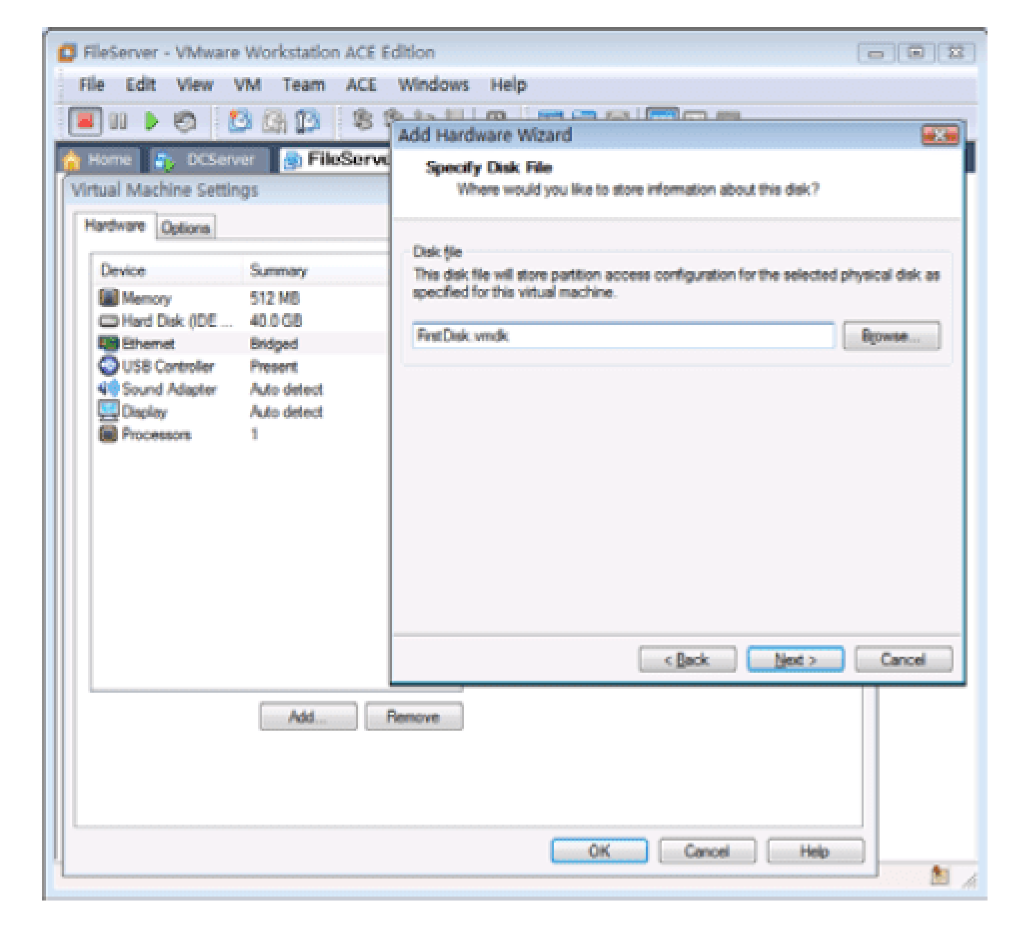




图 11-6　指定磁盘文件

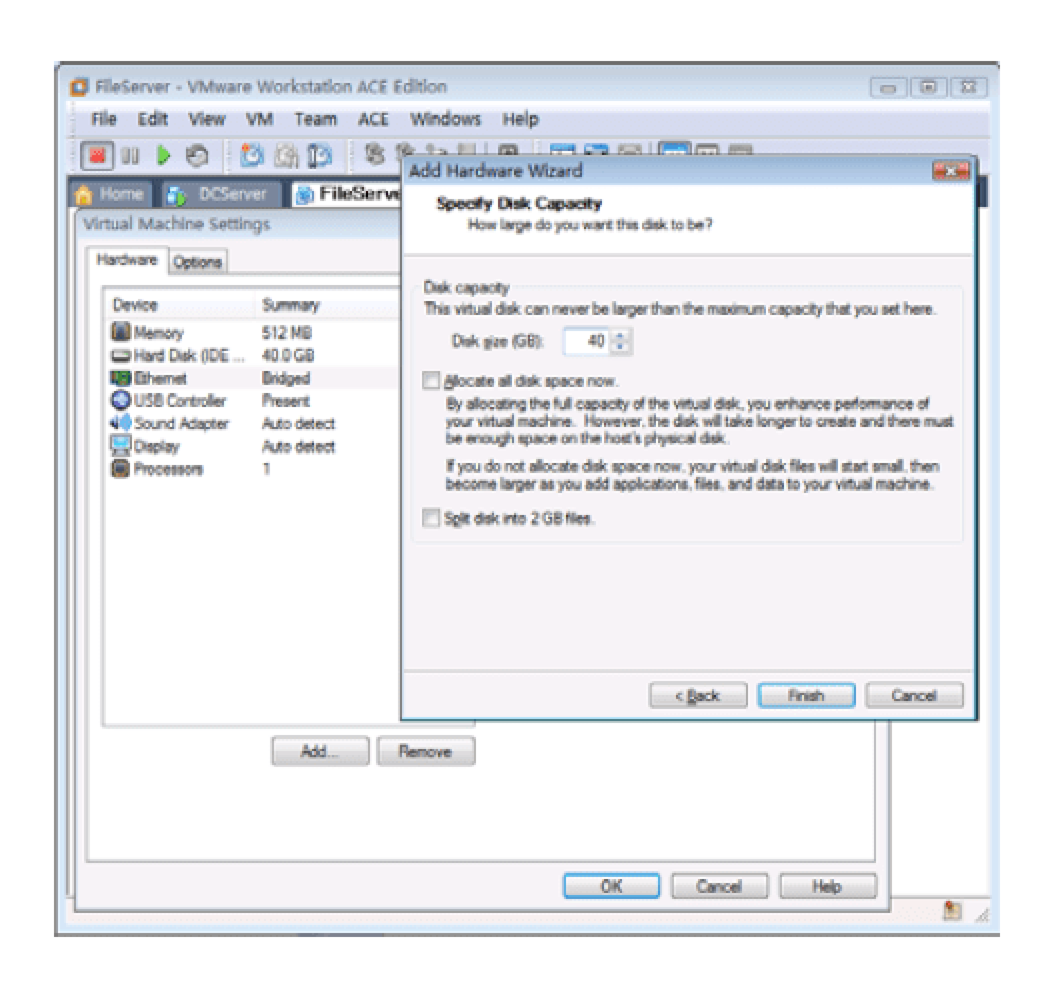


图 11-7　指定磁盘大小

11.2.2　GPT 磁盘类型转换成 MBR 类型

如果初始化磁盘时选择的是 GUID 分区表，在硬盘没有创建分区时，可以将磁盘转换成 MBR 类型。如图 11-8 所示，右击需要转化的磁盘，从弹出的快捷菜单中选择“转换成 MBR 磁盘”命令。

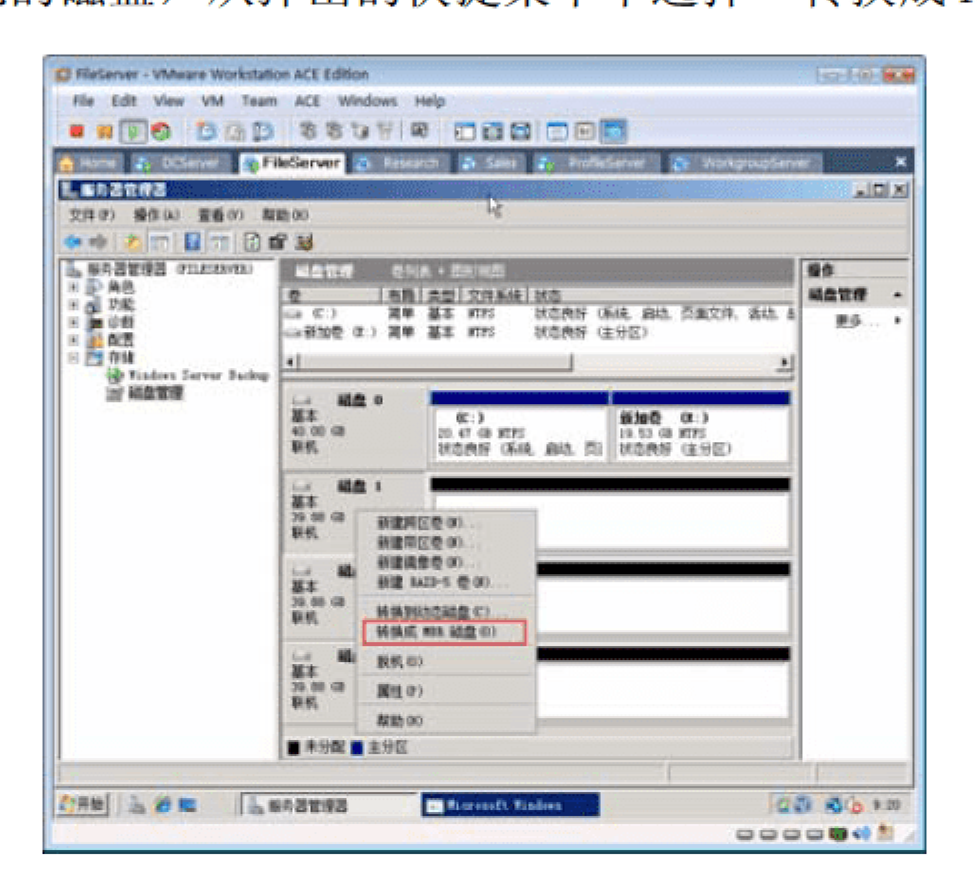


图 11-8　转换成 MBR 磁盘

11.2.3　在 MBR 磁盘上创建分区

在对 MBR 磁盘进行分区之前，有必要理解以下几个基本概念。

- 主磁盘分区。
- 扩展磁盘分区。
- 逻辑驱动器。
- 卷。

1. 主磁盘分区

主磁盘分区是可在基本磁盘上创建的分区类型。主磁盘分区是物理磁盘的一部分，它像物理上独立的磁盘那样工作。对于基本主启动记录(MBR)磁盘，我们可以创建 4 个主分区或 3 个主分区加上一个有多个逻辑驱动器的扩展分区。而对于 GUID 分区表磁盘(GPT)，最多可以创建 128 个主磁盘分区。一个主分区不能再细分，而一个扩展分区可以分成几个逻辑驱动器。

2. 扩展磁盘分区

扩展分区也是一种分区类型，我们只可以在一块基本的主启动(MBR)磁盘上创建扩展分区。如果我们想在基本的 MBR 磁盘上创建 4 个以上的卷，使用扩展磁盘分区将非常有用。与主磁盘分区不同，我们不要用一个文件系统来格式化一个扩展分区，然后给它指派一个逻辑驱动器。相反，可以在一个扩展分区上创建多个逻辑驱动器，然后再用文件系统对它们进行格式化。

3. 逻辑驱动器

逻辑驱动器就是在基本主启动记录(MBR)磁盘的扩展磁盘中创建的卷。逻辑驱动器类似于主磁盘分区，只是在每个磁盘中最多只能有 4 个主分区，而在每个磁盘上创建的逻辑驱动器的数目可以达到 24 个。在 GUID 分区表磁盘上不能创建扩展分区或逻辑驱动器。

示例：在 MBR 磁盘上创建分区。

① 如图 11-9 所示，右击磁盘 1 未分配空间，从弹出的快捷菜单中选择“新建简单卷”命令。



提示：在 Windows Server 2008 中，在静态磁盘上创建简单卷等同于早期版本的分区。

② 打开新建简单卷向导，单击“下一步”按钮。

③ 如图 11-10 所示，在出现的“指定卷大小”对话框中输入 2000，单击“下一步”按钮。

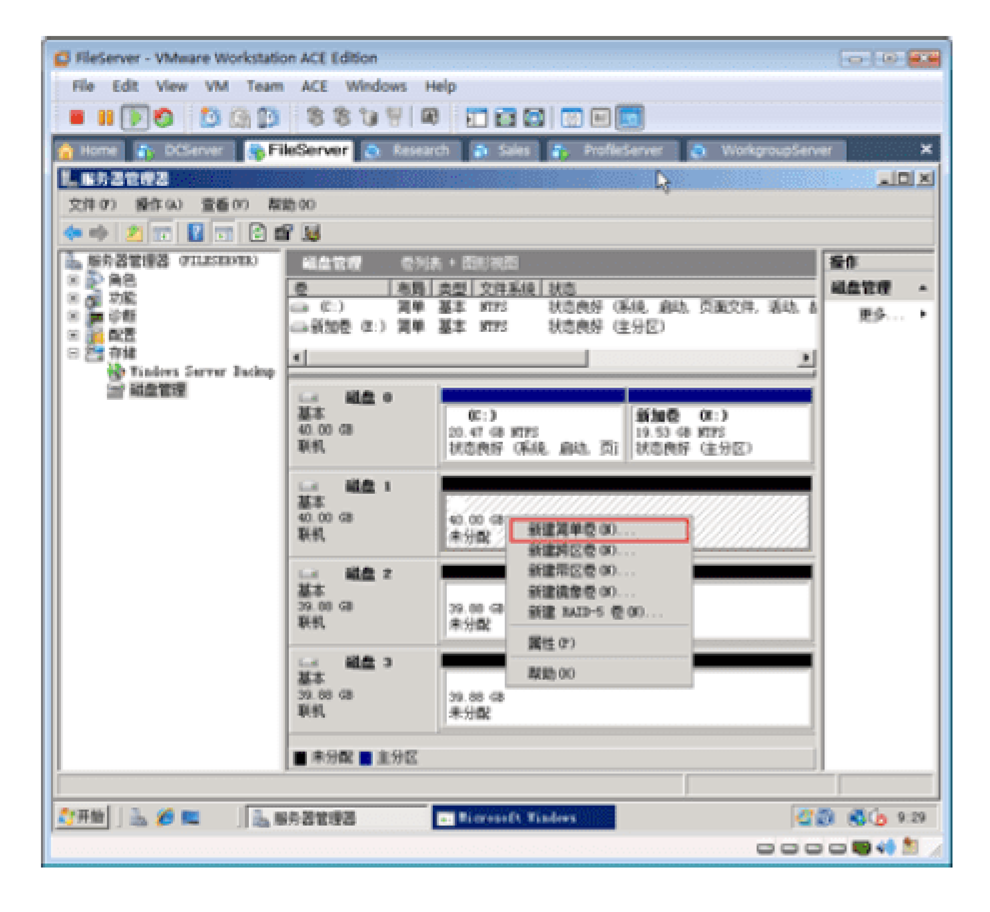


图 11-9　创建简单卷

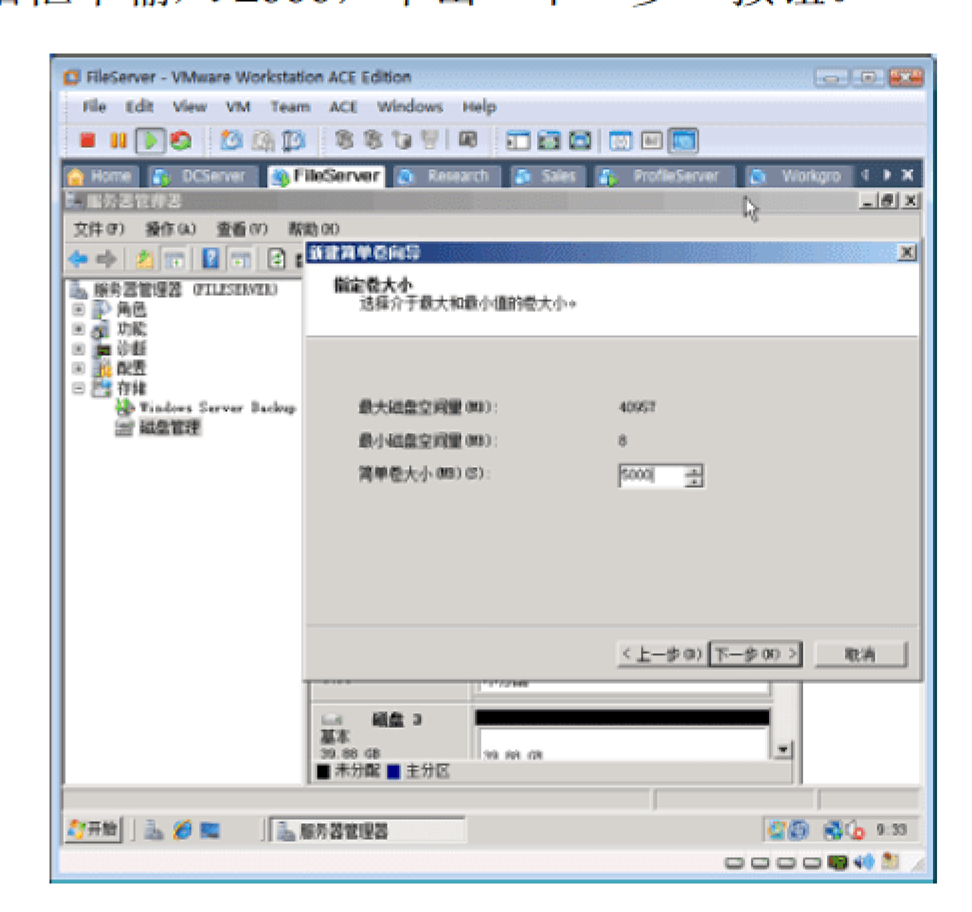


图 11-10　指定大小

④ 如图 11-11 所示，在出现的“分配驱动器号和路径”界面中，指定盘符，单击“下一步”按钮。

⑤ 如图 11-12 所示，在出现的“格式化分区”界面中，选定文件系统为 NTFS，选中“执行快速格式化”复选框，单击“下一步”按钮。

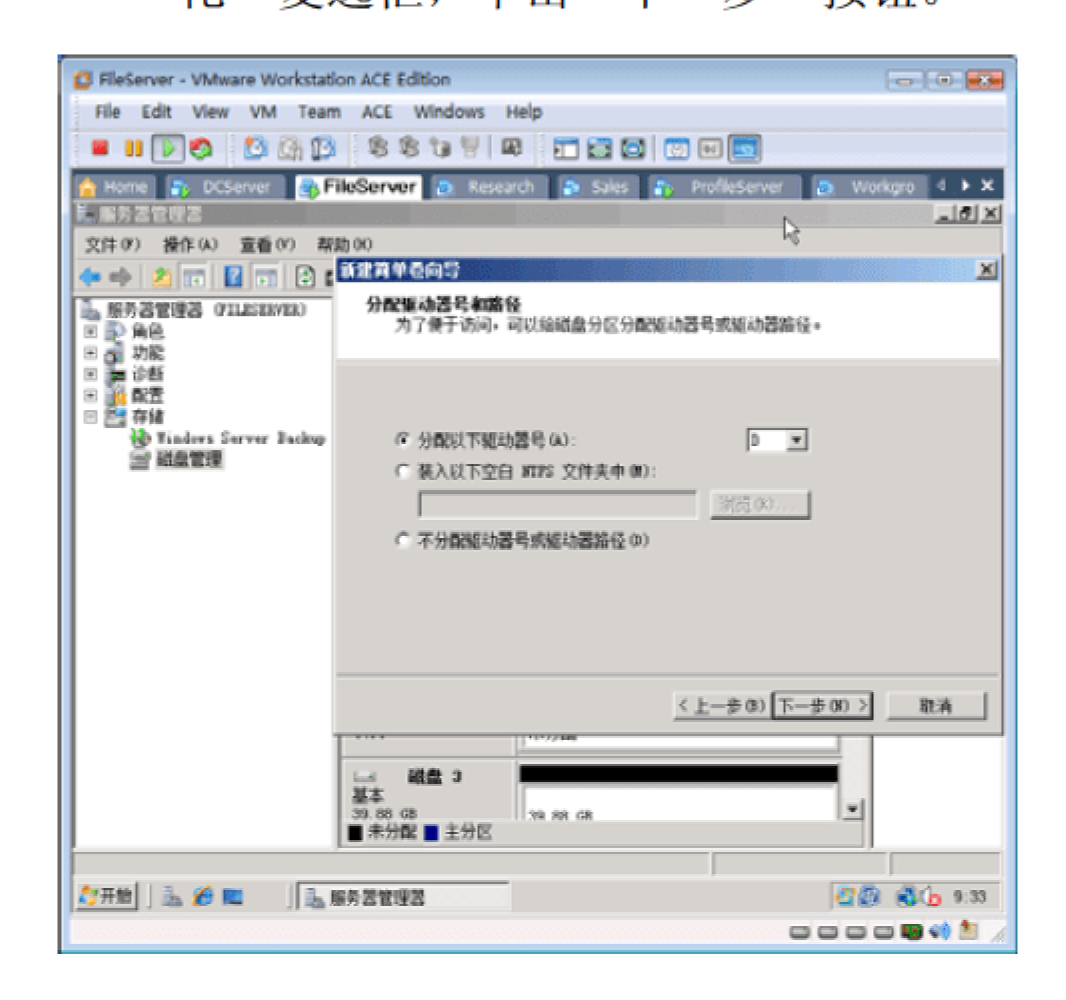


图 11-11　指定盘符和路径

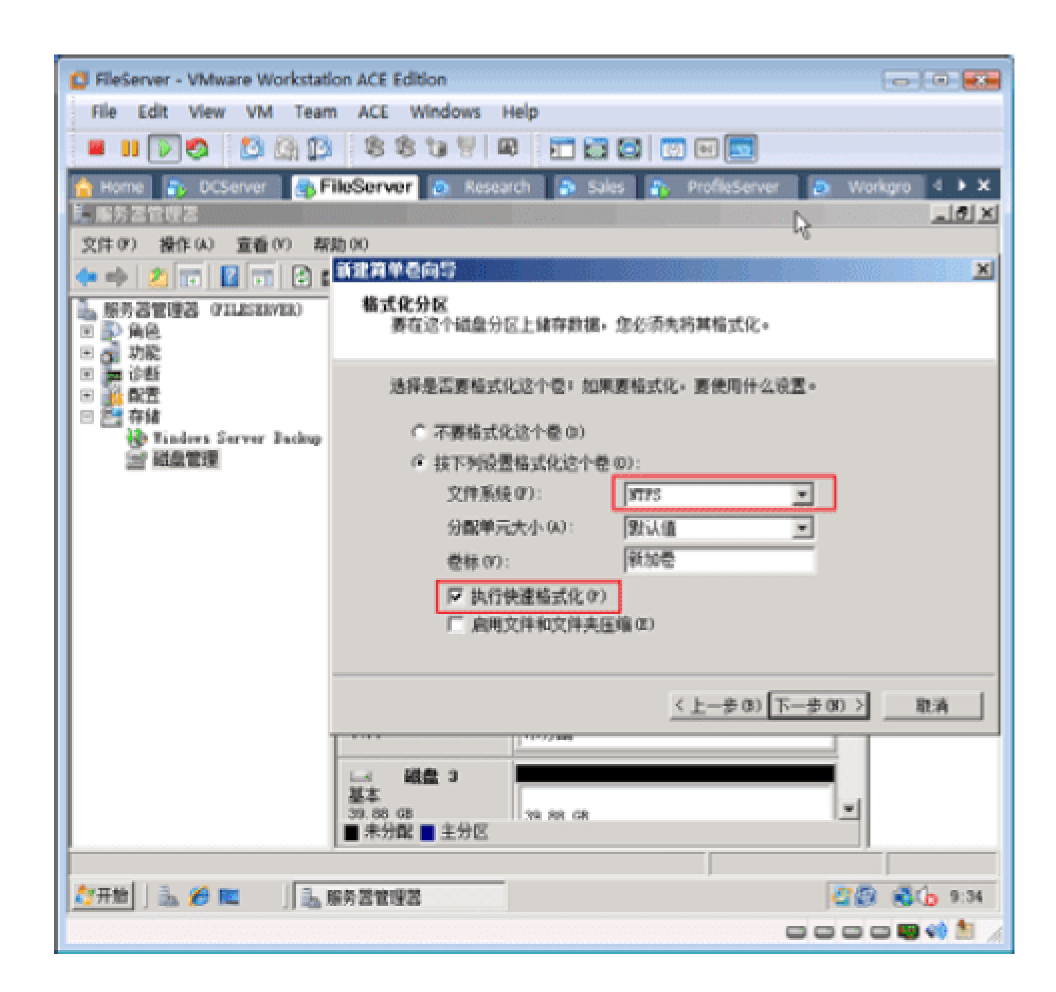


图 11-12　格式化分区

⑥ 如图 11-13 所示，如果创建的简单卷超过 3 个，则可以看到第四个卷将会自动放在扩展分区上。

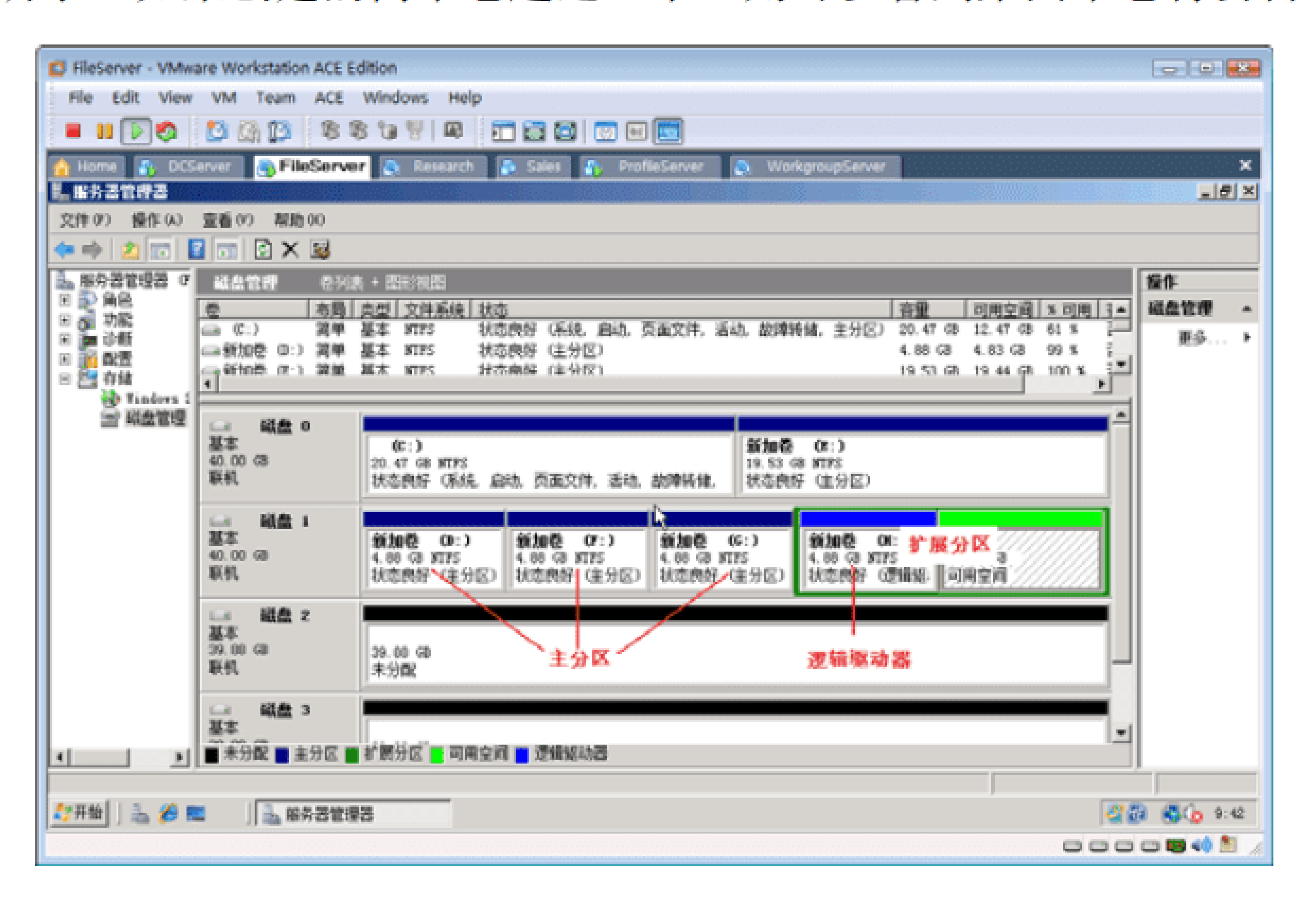


图 11-13　扩展分区

11.2.4　磁盘属性概述

磁盘的属性提供了有关磁盘的最近信息。我们可以使用 DiskPart 命令行工具或 Disk Management 磁盘属性对话框来访问其属性信息。

① 如图 11-14 所示，右击磁盘，从弹出的快捷菜单中选择“属性”命令。

② 如图 11-15 所示，在“常规”选项卡中，我们可以了解该磁盘设备的类型、制造商和位置等信息。

③ 磁盘属性对话框的“卷”选项卡如图 11-16 所示。通过“卷”选项卡，我们可以了解磁盘的编号、类型、状态、磁盘分区形式、容量、未分配空间和保留空间等信息。

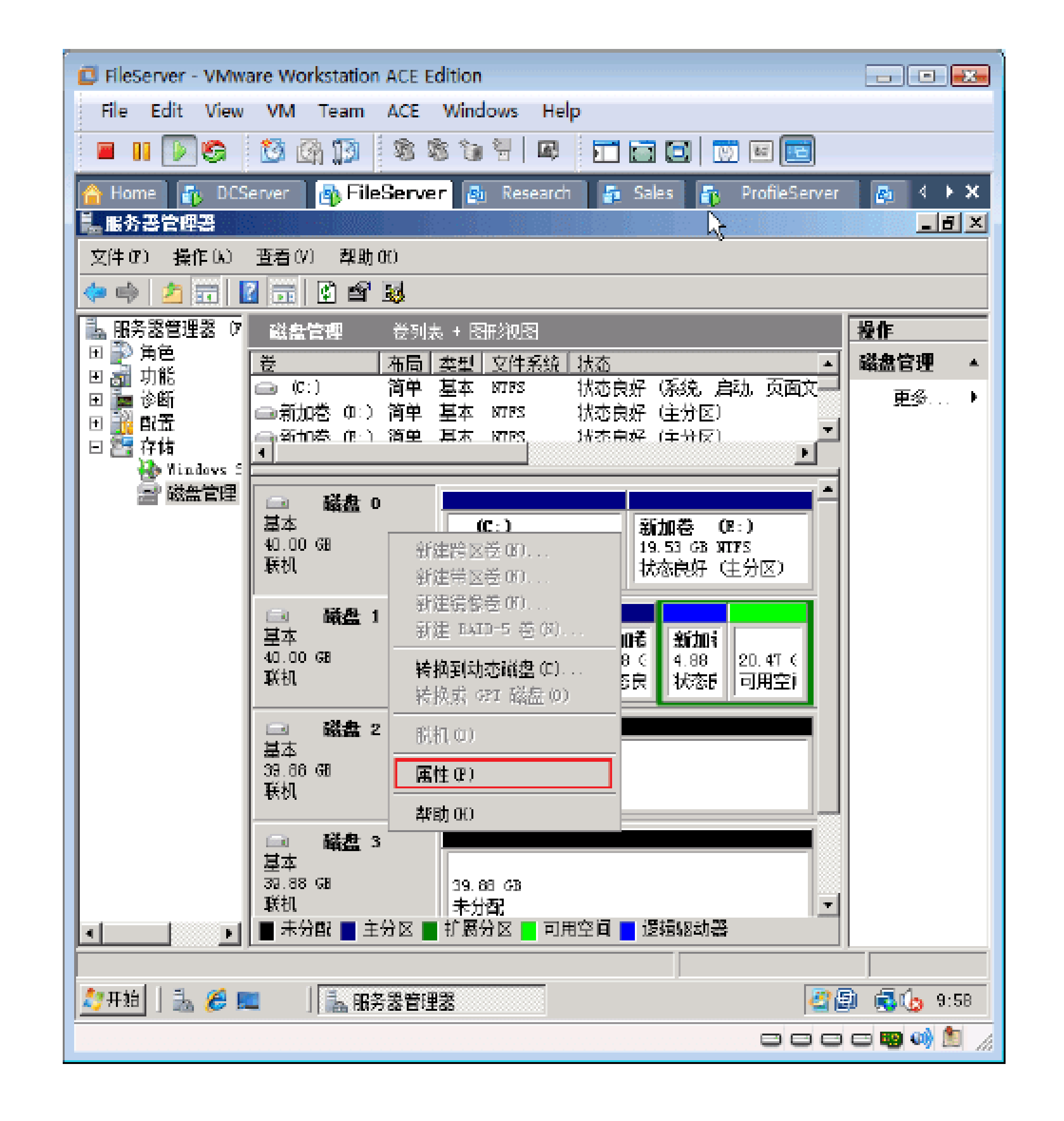


图 11-14　磁盘属性

图 11-15　磁盘信息

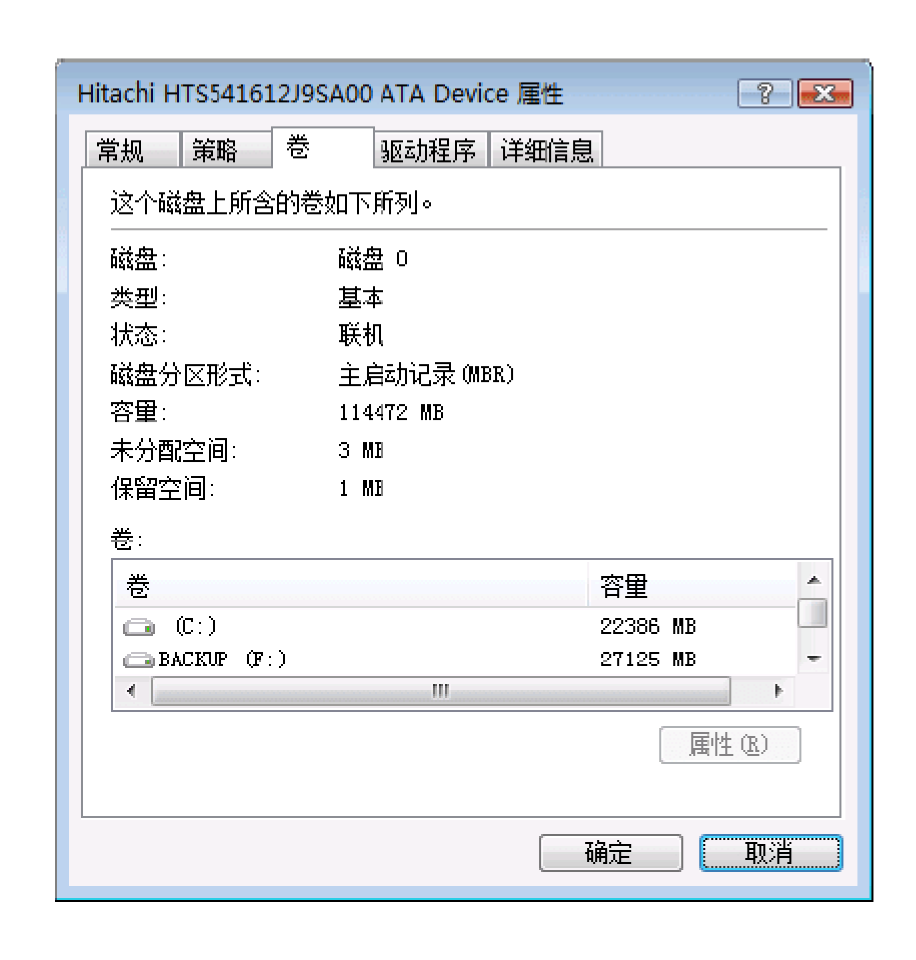


图 11-16　卷的信息

11.2.5　重新扫描磁盘

当在计算机之间移动硬盘之后，必须重新扫描磁盘。当重新扫描磁盘属性时，它将扫描所有的硬盘，以及磁盘配置信息的改变。通过重新扫描磁盘还可以更新可移动存储媒体、CR-ROM 驱动器、基本卷、文件系统和驱动器号。

当我们在计算机中安装一块新硬盘，而 Disk Management 却没有检测到该硬盘时，可以通过重新扫描该硬盘来更新硬盘的属性。

如图 11-17 所示，右击“磁盘管理”选项，从弹出的快捷菜单中选择“重新扫描磁盘”命令。

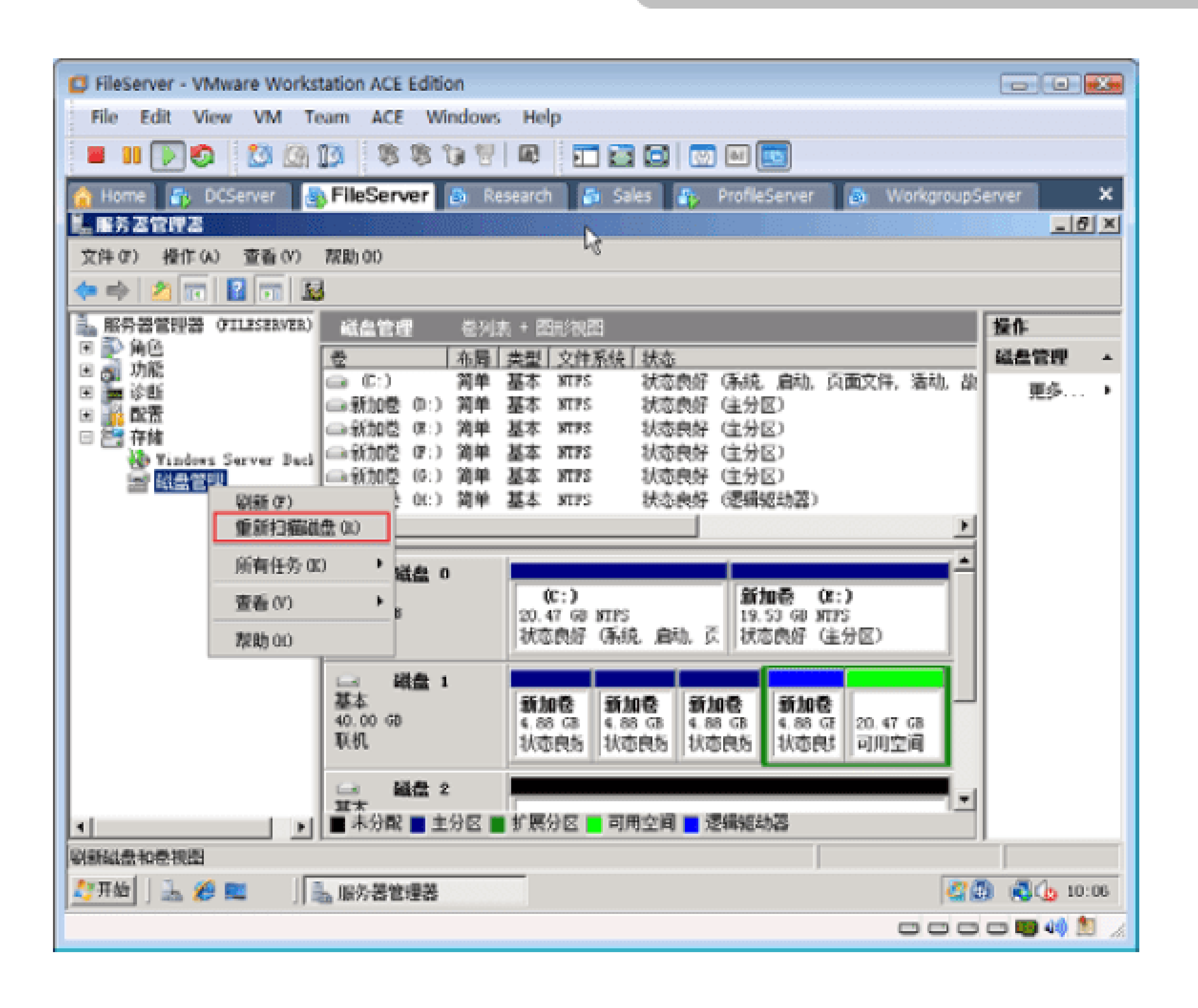


图 11-17　重新扫描磁盘

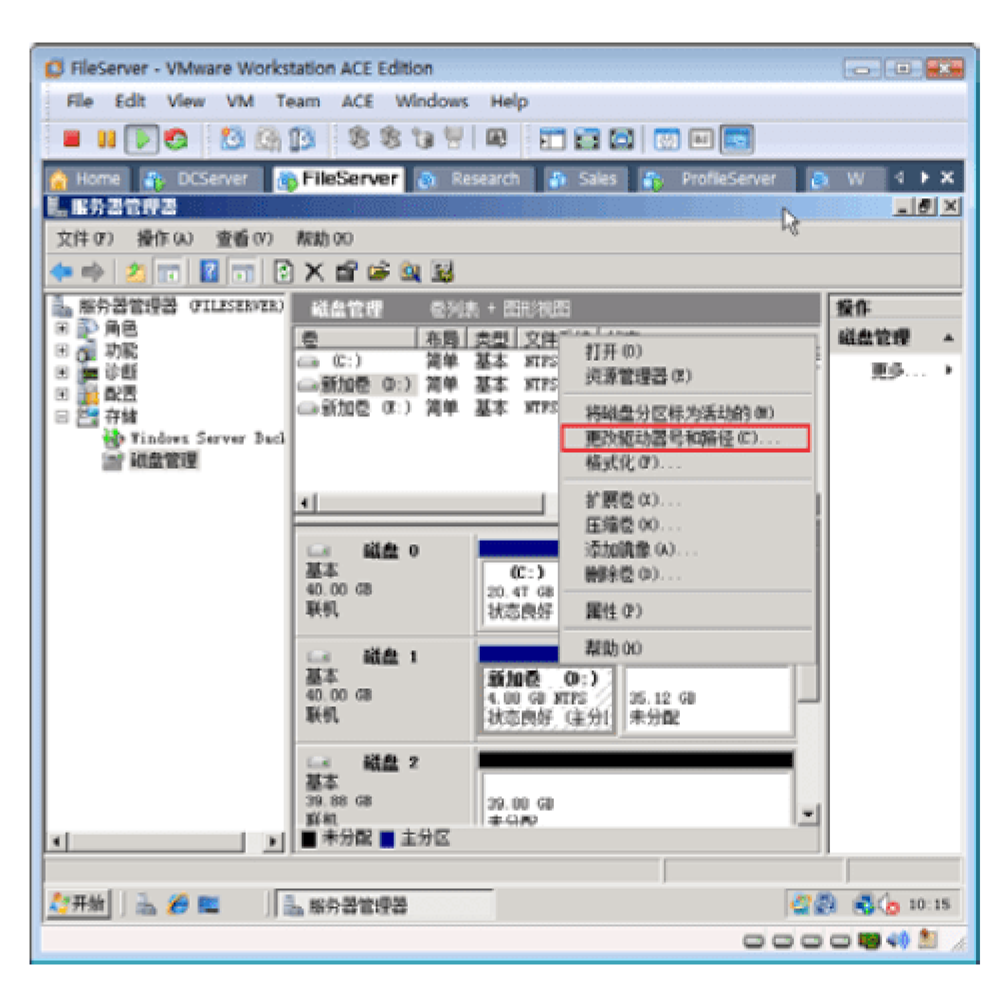
11.3　更改驱动器号和路径

11.3.1　更改驱动器号

在创建卷时指定的驱动器号，在使用了一段时间后还可以根据需要进行更改。

① 如图 11-18 所示，右击卷，从弹出的快捷菜单中选择“更改驱动器号和路径”命令。

② 如图 11-19 所示，在出现的对话框中，单击“更改”按钮。在出现的对话框中，选定盘符，单击“确定”按钮。



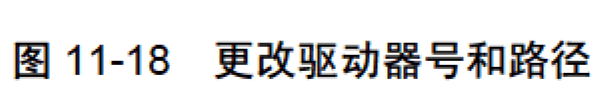


图 11-18　更改驱动器号和路径

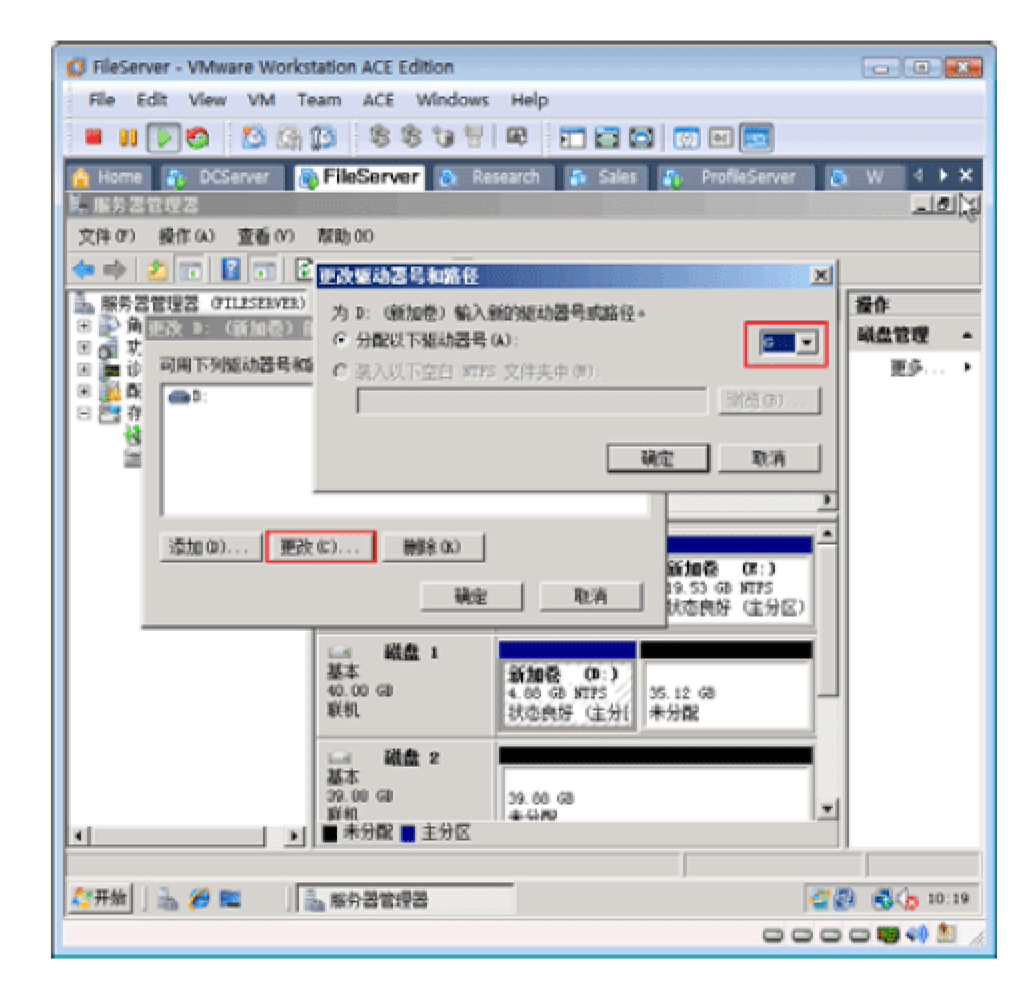


图 11-19　更改盘符

③ 如图 11-20 所示，在出现的“磁盘管理”提示对话框中，单击“是”按钮。

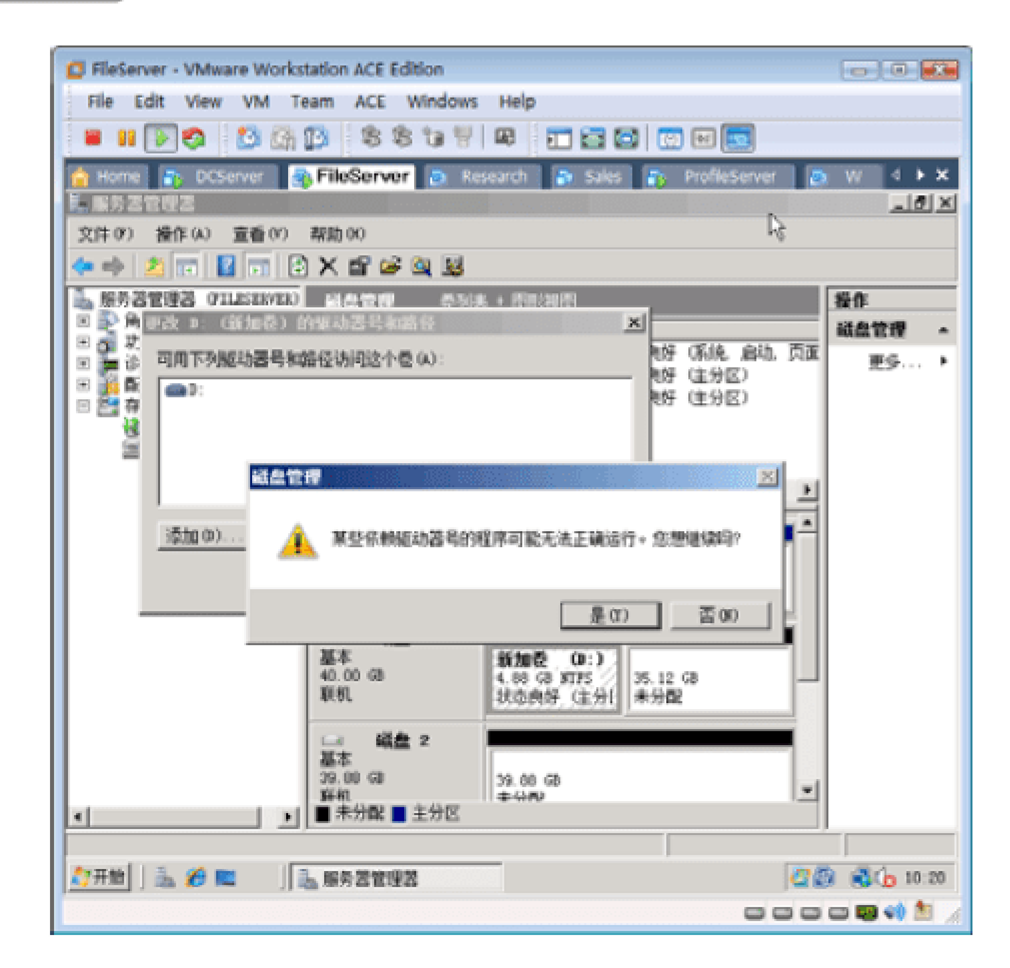


图 11-20　更改盘符

11.3.2　挂接卷

我们可以将磁盘分区或卷挂接到空的 NTFS 文件下，用户可以通过该文件夹访问磁盘分区。

① 如图 11-21 所示，右击卷，从弹出的快捷菜单中选择“更改驱动器号和路径”命令。

② 如图 11-22 所示，在出现的“更改”对话框中单击“添加”按钮。

③ 如图 11-22 所示，在出现的“添加驱动器号或路径”对话框中，单击“浏览”按钮，选定 C:\，单击“新建文件夹”按钮，输入“G 盘”，单击“确定”按钮。

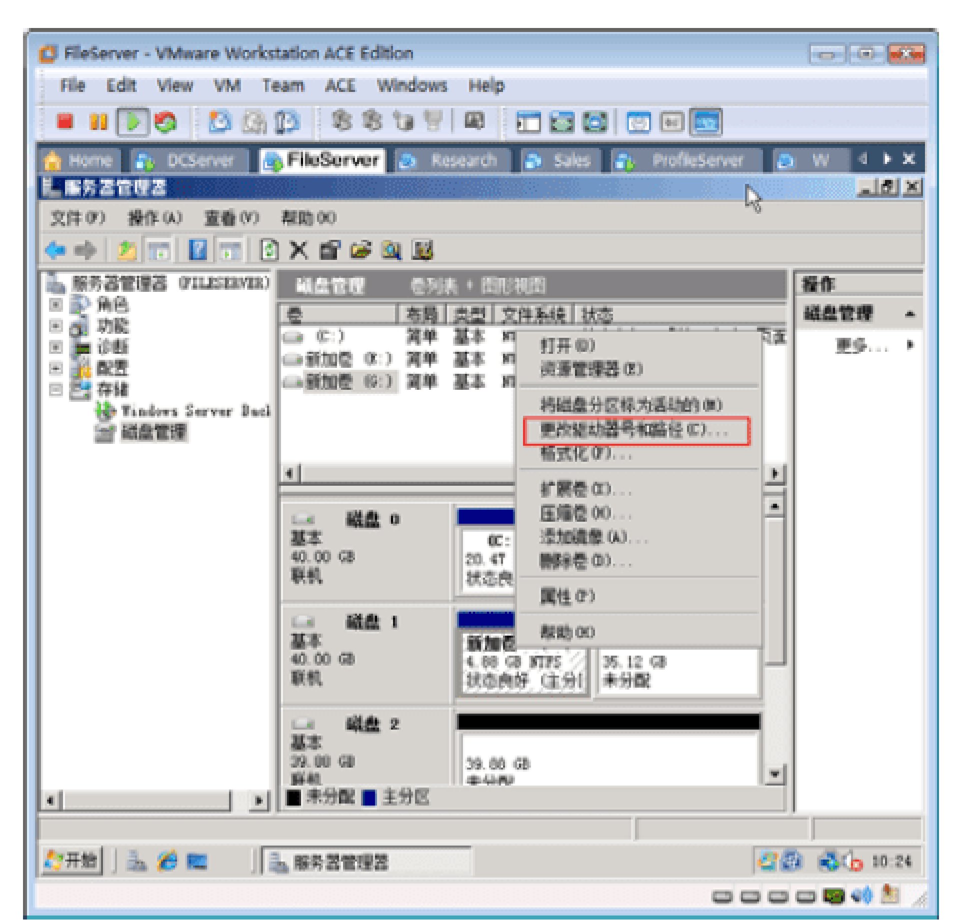
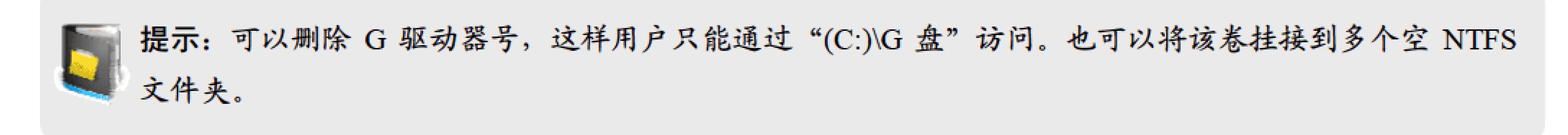


图 11-21　更改盘符和路径

图 11-22　挂接到空 NTFS 文件夹

④ 如图 11-23 所示，可以看到，除了 G 驱动器之外，还可以用(C:)\G 盘访问这个卷。



提示：可以删除 G 驱动器号，这样用户只能通过“(C:)\G 盘”访问。也可以将该卷挂接到多个空 NTFS 文件夹。

⑤ 如图 11-24 所示，打开(C：)盘，可以看到有一个使用磁盘图标的文件夹“G 盘”。单击 G 盘，可

以打开 G 卷。

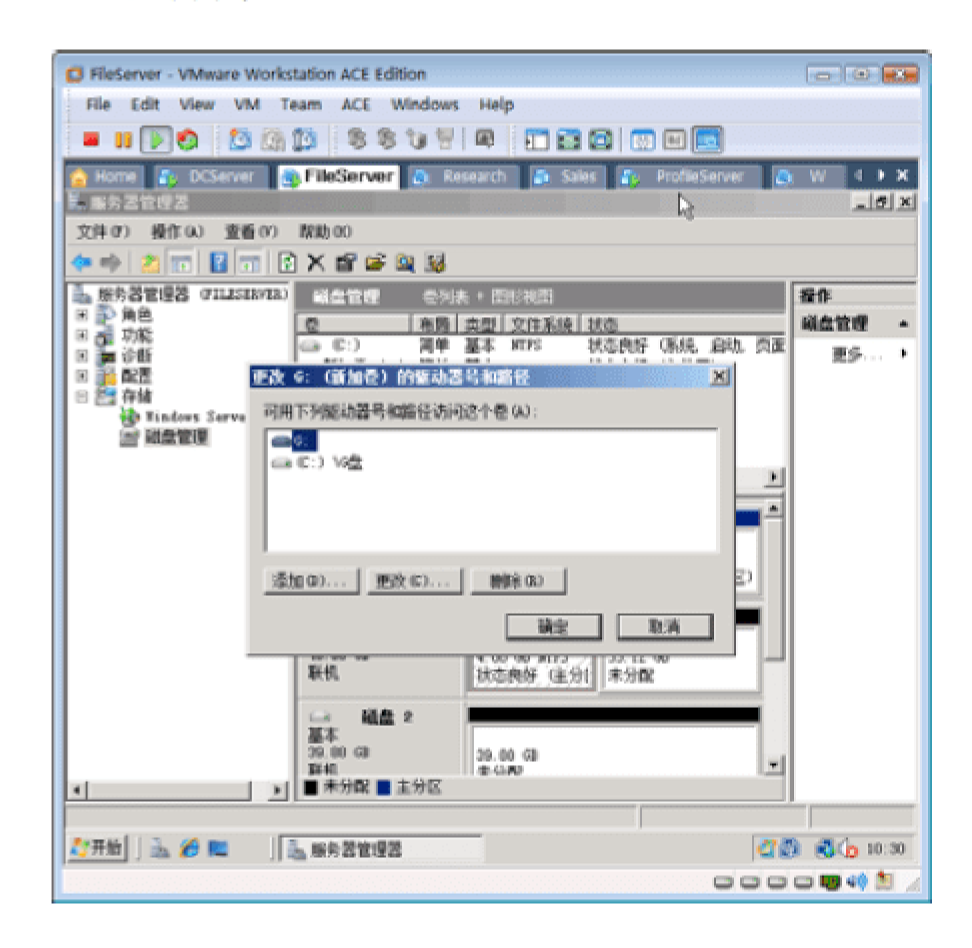



图 11-23　挂接卷

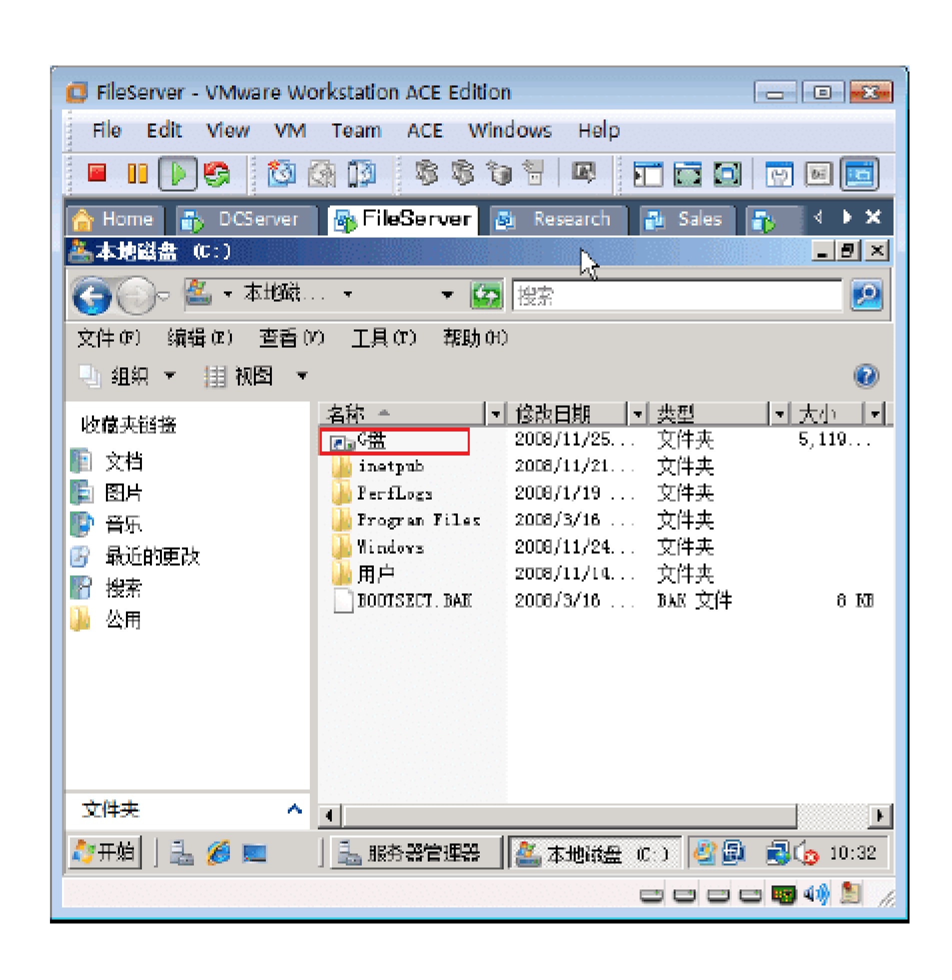


图 11-24　查看挂接卷

什么时候使用挂接卷

装入的驱动器不受 26 个驱动器号限制的影响，因此可以使用装入的驱动器在计算机上访问 26 个以上的驱动器，驱动器号紧张时使用挂接卷。

如果你使用的程序在开发时指定使用系统目录下的 downloads 文件夹并且不能更改，而系统盘空间不够用，可以将一个新卷挂接到 download 文件夹。

11.4　实现磁盘转换

11.4.1　基本磁盘与动态磁盘

基本磁盘是 Windows Server 2008 默认的磁盘类型。基本磁盘是包含主磁盘分区、扩展磁盘分区或逻辑驱动器的物理磁盘。基本磁盘上的分区和逻辑驱动器称为基本卷，只能在基本磁盘上创建基本卷。使用基本磁盘的好处在于，它可以提供单独的空间来组织数据。

可在基本磁盘上创建的分区个数取决于磁盘的分区样式。

- 对于主启动记录(MBR)磁盘，可以最多创建四个主磁盘分区，或最多三个主磁盘分区加上一个扩展分区。在扩展分区内，可以创建多个逻辑驱动器。
- 对于 GUID 分区表 (GPT) 磁盘，最多可创建 128 个主磁盘分区。由于 GPT 磁盘并不限制四个分区，因而不必创建扩展分区或逻辑驱动器。

动态磁盘可以提供基本磁盘所不具备的一些功能，例如创建可跨越多个磁盘的卷和创建具有容错能力的卷，所有动态磁盘上的卷都是动态卷。在动态磁盘中可以创建五种类型的动态卷：简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷，其中镜像卷和 RAID-5 卷是容错卷。

使用动态磁盘的好处在于以下方面。

- 动态磁盘可被用来创建跨越多个磁盘的卷。

- 动态磁盘可被用来创建默认的容错磁盘，以确保当硬件发生故障时的数据完整性。
- 在每个动态磁盘上可以创建最多 2000 个动态卷，但是动态卷的推荐值是 32 个或更少。

在 Windows Server 2008 中我们可以实现基本磁盘与动态磁盘之间的相互转换。将基本磁盘转换成动态磁盘可以实现以下功能。

- 创建或删除简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷。
- 扩展一个简单卷或跨区卷。
- 修复镜像卷或 RAID-5 卷。
- 使跨越多个磁盘的卷恢复活动。

我们可以在任何时间将基本磁盘转换成动态磁盘，而不会丢失数据。当将一个基本磁盘转换成动态磁盘时，在基本磁盘上的分区将变成卷。我们也可以将动态磁盘转换成基本磁盘，但是在动态磁盘上的数据将会丢失。为了将动态磁盘转换成基本磁盘，要先删除动态磁盘上的数据和卷，然后从未分配的磁盘空间上重新创建基本分区。

表 11-1 对比了基本磁盘与动态磁盘之间的差异。

表 11-1　基本磁盘与动态磁盘

磁　盘	好　处
基本磁盘	使用所创建的独立的空间组织数据 可以被划分成 4 个主分区或 3 个主分区和一个扩展分区
动态磁盘	使用跨越多个磁盘的卷 每块磁盘上的卷的数目不受限制 使用所创建的默认的容错磁盘确保数据的完整性

11.4.2　将基本磁盘转换为动态磁盘

大多数组织在他们的服务器中都使用动态磁盘。通过使用动态磁盘一方面可以提供默认的容错，另一方面可以在需要的时候扩展磁盘空间。在 Windows Server 2003 中默认的磁盘类型是基本磁盘，如果我们计划使用动态磁盘，必须将一个基本磁盘转换成动态磁盘。

将基本磁盘转换成动态磁盘后，动态磁盘将既不包含基本卷(主磁盘分区或逻辑驱动器)，也不能由 MS-DOS、Windows 95、Windows 98、Windows Millennium Edition、Windows NT 或 Windows XP Home Edition 操作系统访问。只有 Windows 2000、Windows XP Professional、Windows Server 2003 或 Windows Server 2008 家族操作系统才能访问动态卷。将基本磁盘转换为动态磁盘之后，基本磁盘上已有的全部分区或逻辑驱动器都将变为动态磁盘上的简单卷。

示例：将基本磁盘转换为动态磁盘。

① 如图 11-25 所示，右击磁盘，从弹出的快捷菜单中选择“转换到动态磁盘”命令。

② 如图 11-26 所示，在出现的“转换为动态磁盘”对话框中，选中要转换的磁盘，单击“确定”按钮。

注意：将基本磁盘转化为动态磁盘后，不能将动态卷改回到分区，而必须先删除磁盘上的所有动态卷，然后使用降级成基本磁盘。如果要保留数据，必须将数据备份或转移到另一个卷上。

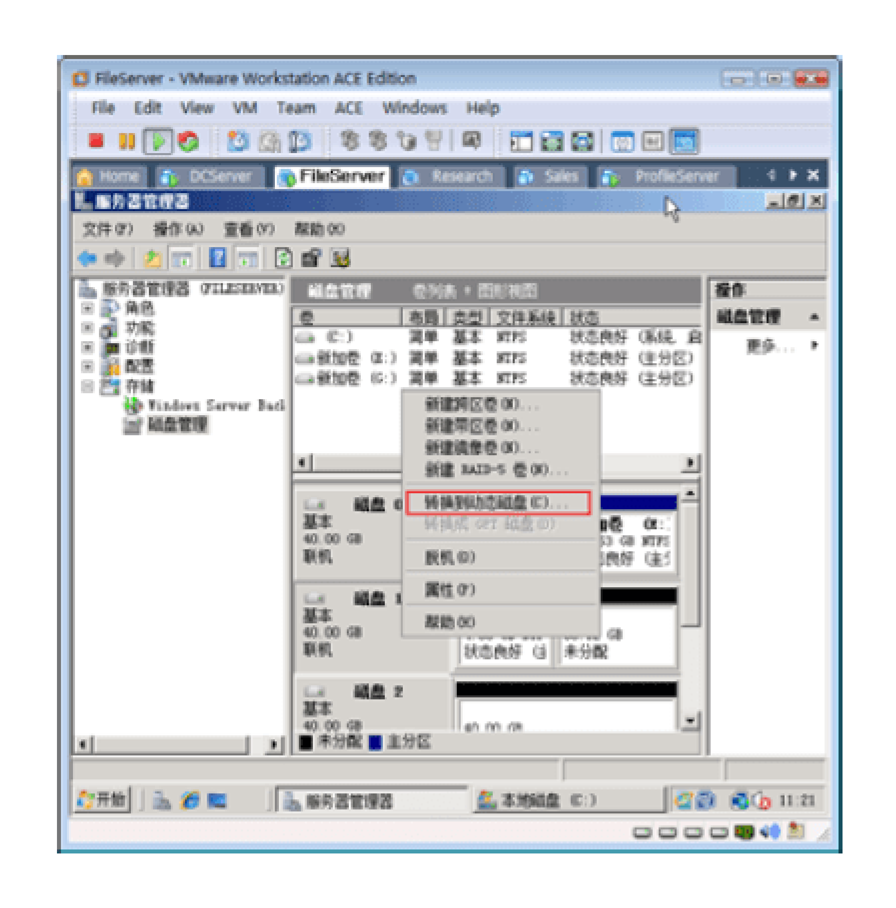


图 11-25　转换成动态磁盘

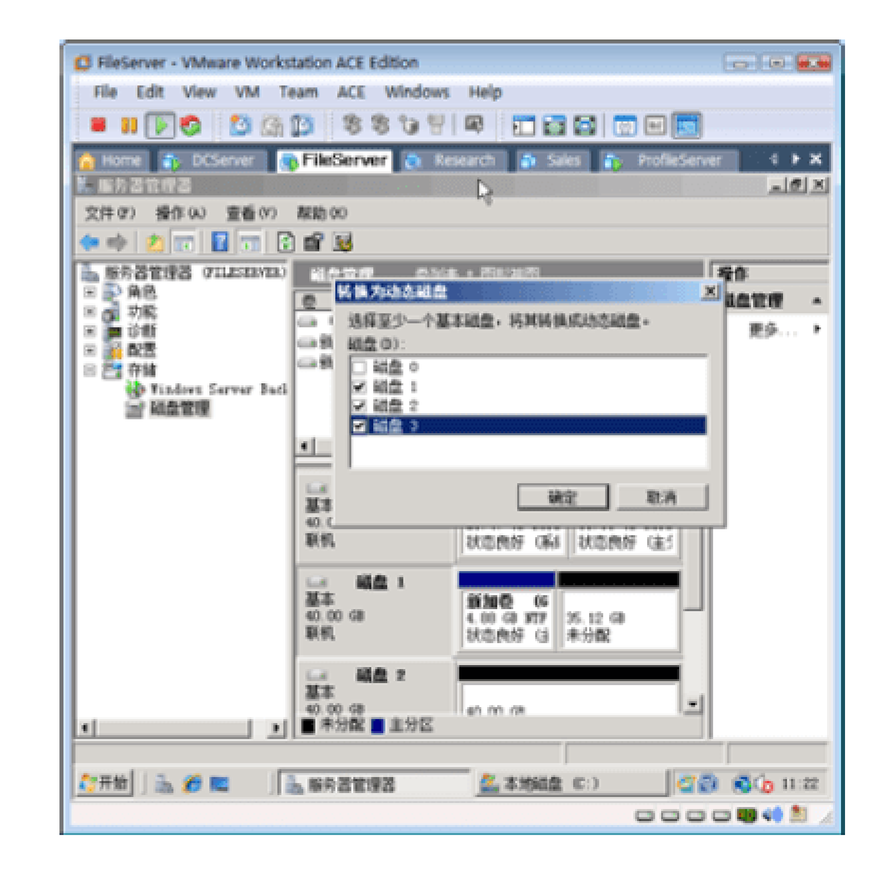


图 11-26　选择要转换的磁盘

③　如图 11-27 所示，在出现的“要转换的磁盘”对话框中单击“转换”按钮。

④　如图 11-28 所示，在出现的提示对话框中单击“是”按钮。

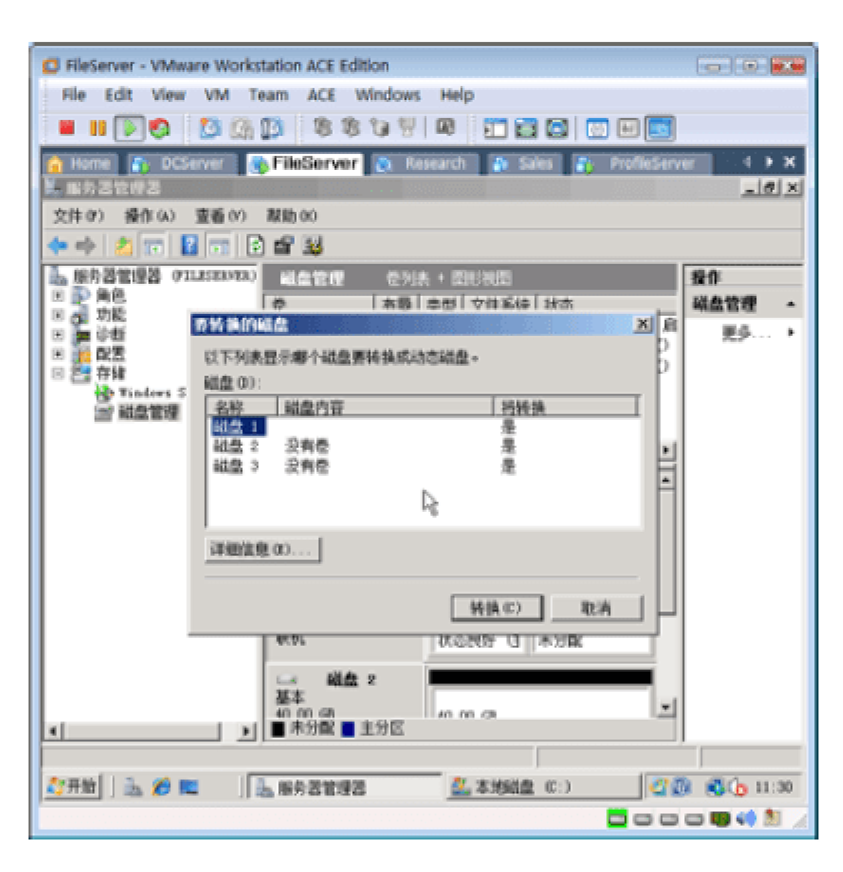


图 11-27　要转换的磁盘

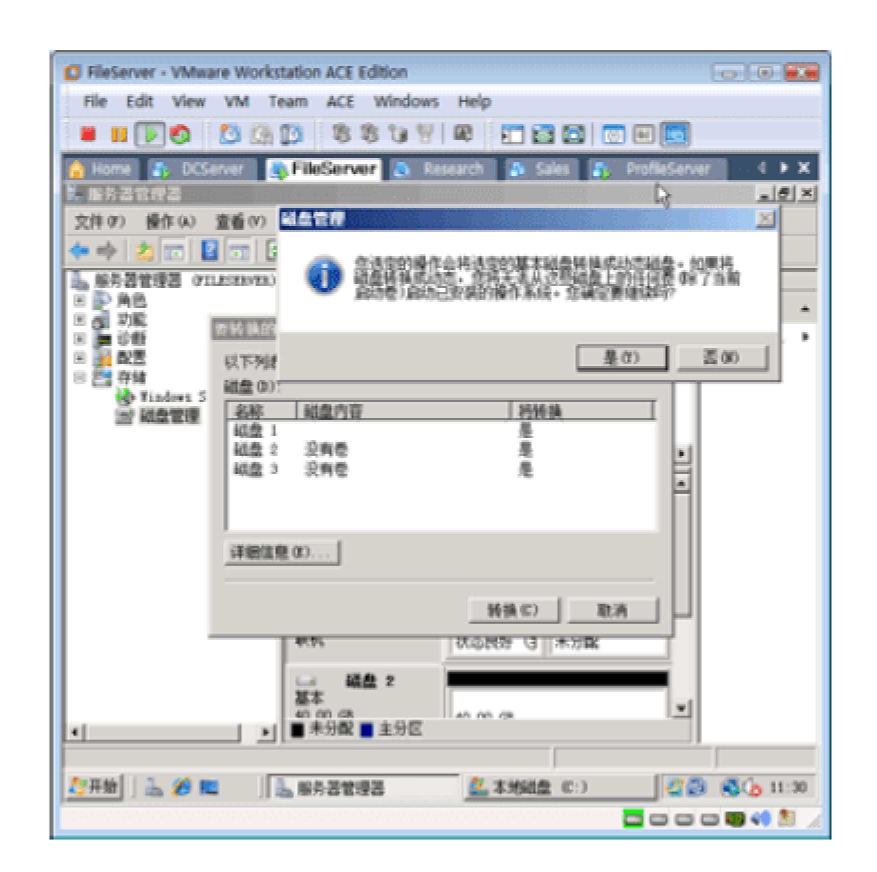


图 11-28　磁盘转换

⑤　如图 11-29 所示，可以看到将基本磁盘转换成动态磁盘，分区的内容不会丢失。

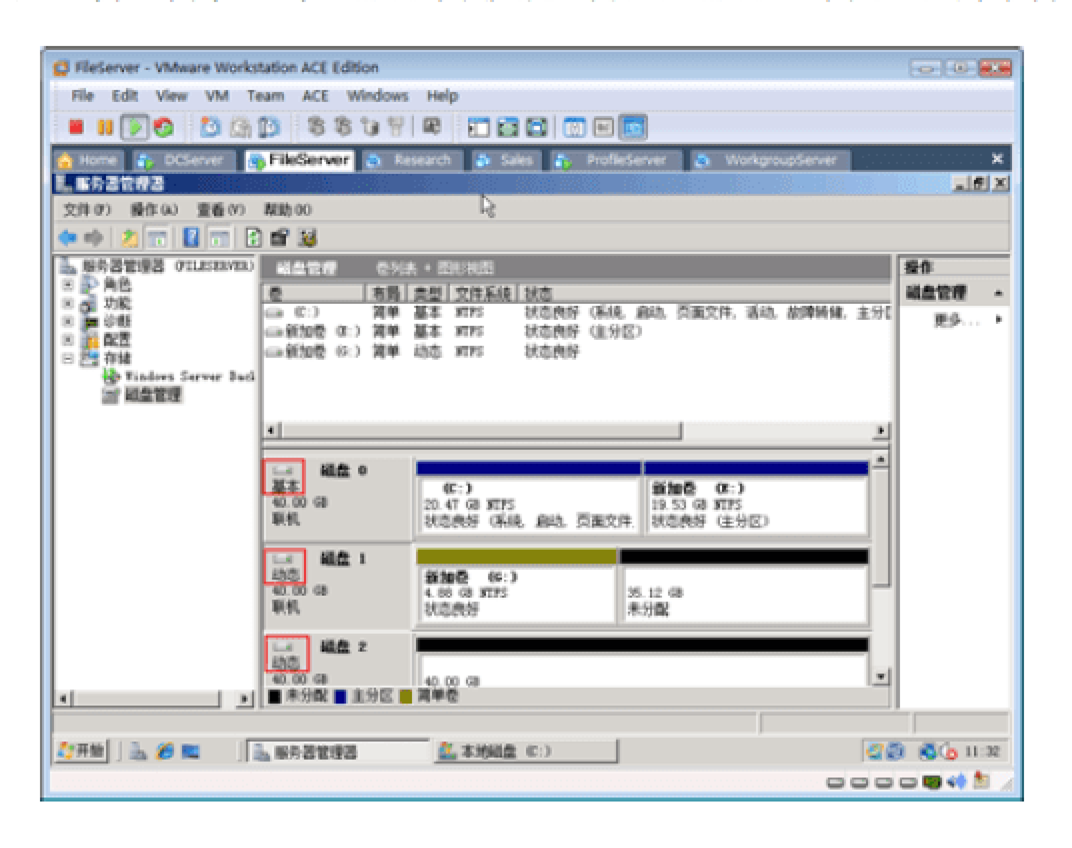


图 11-29　动态磁盘

11.4.3 将动态磁盘转换为基本磁盘

在将动态磁盘转换回基本磁盘之前，在该动态磁盘上绝不能具有任何卷，也不能包含任何数据。如果要保存数据，则在转化磁盘之前应备份该磁盘上的数据，或将其转移到另一个卷上。

如图 11-30 所示，没有卷的硬盘可以转换成基本磁盘。如图 11-31 所示，如果动态磁盘有卷，将不可转换成基本磁盘。

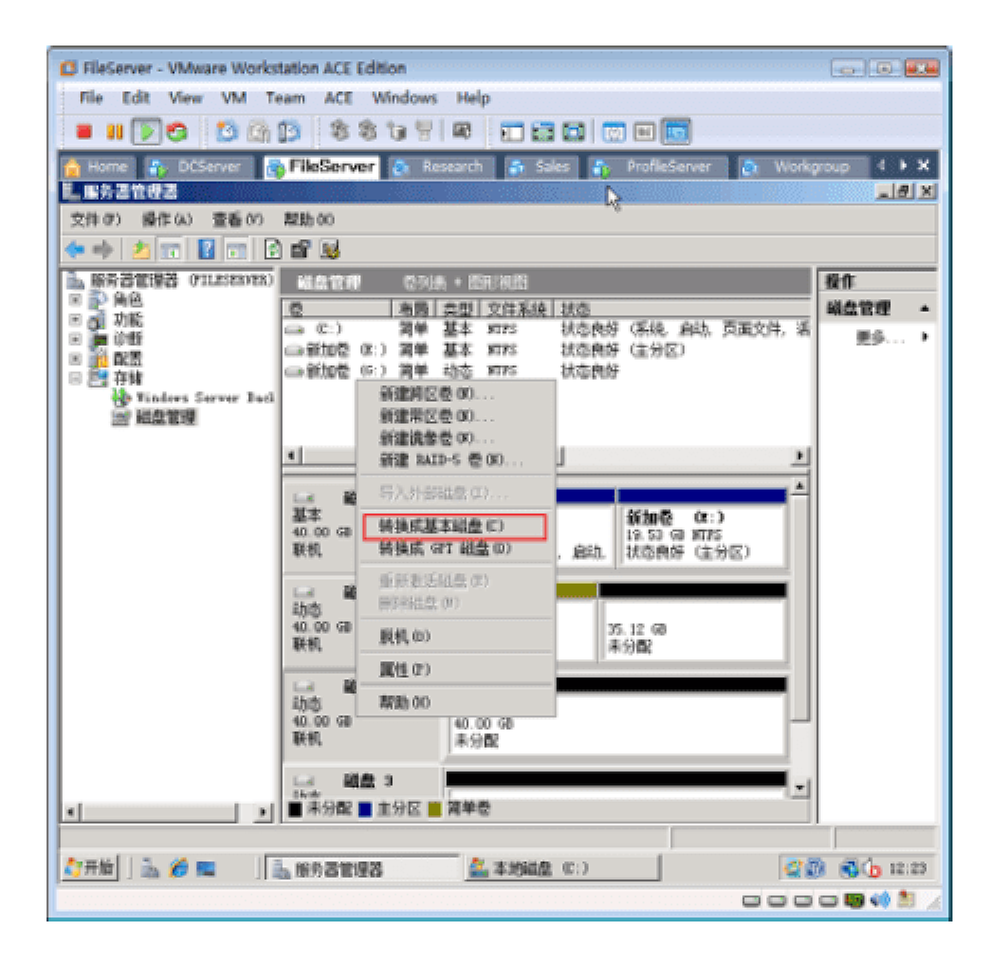


图 11-30 转换成基本磁盘

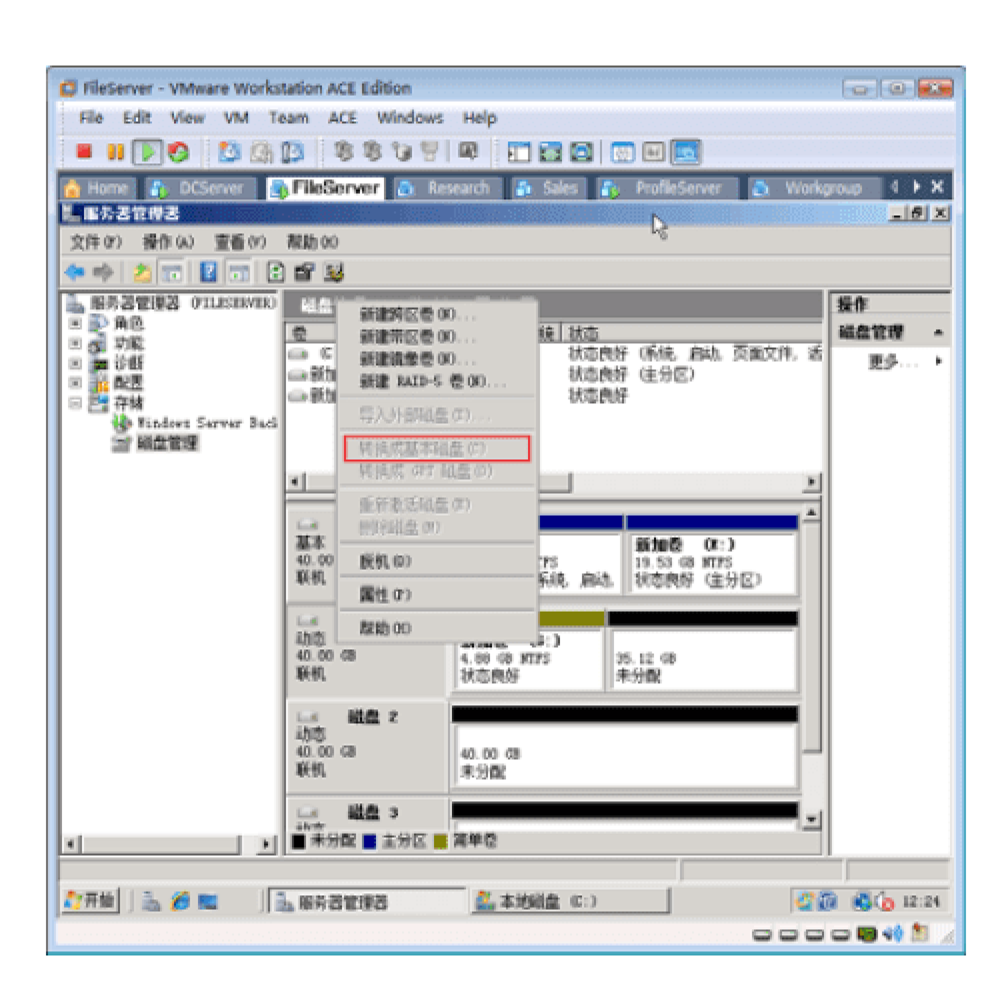


图 11-31 不能转换

11.5 管理动态卷

在动态磁盘上我们可以创建卷，卷就是磁盘上的存储区域。一个硬盘可以有多个卷，一个卷也可以跨越多个磁盘。我们可以使用一种文件系统来格式化卷，并给卷指派一个驱动器号。

11.5.1 卷的类型

1. 简单卷

一个简单卷就是驻留在一个动态磁盘上的单一的卷。简单卷是物理磁盘的一部分，但它工作时就好像是物理磁盘上的一个独立单元。我们可以从动态磁盘的未分配空间来创建简单卷，但当只有一个动态磁盘时，简单卷是我们可以创建的唯一卷。简单卷与分区相似，但与分区不同，简单卷既没有大小限制，也没有在一块磁盘上可创建卷的数目的限制。

在简单卷中可以使用的文件系统包括：NTFS、FAT 和 FAT32。我们可以通过将卷扩展到相同或不同磁盘上的未分配空间上来增加现有简单卷的大小。要扩展简单卷，则该卷必须尚未格式化，可以通过 Windows 2003 或 Windows Server 2008 系列操作系统中使用的 NTFS 版本对卷进行格式化。在 Windows Server 2008 系列操作系统上，可以扩展简单卷，除非该卷是系统分区、启动分区或以前是基本磁盘上的分区的简单卷，这些基本磁盘已经通过 Windows 2008 转换为动态磁盘。扩展相同磁盘上的简单

卷后，该卷仍为简单卷，且仍然可以镜像它。

只有 Windows 2000、Windows XP Professional、Windows Server 2003 和 Windows Server 2008 家族操作系统才能访问简单卷。如果计算机上还运行 MS-DOS、Windows 95、Windows 98、Windows Millennium Edition、Windows NT 4.0 或 Windows XP Home Edition 等，则应该在基本磁盘上创建基本卷，因为这些操作系统不能访问动态卷。

可以使用简单卷来实现所有的数据存储，直到在磁盘空间不足。为了获得更多的磁盘空间，可以创建一个扩展的、跨区的、带区的卷。

2. 跨区卷

使用跨区卷可以将来自多个磁盘的未分配空间合并到一个逻辑卷中，这样我们可以更有效地使用多个磁盘系统上的所有空间和所有驱动器号。在一个卷被扩展之后，为了删除扩展卷的一部分，我们必须删除整个跨区卷。

跨区卷具有以下几个特点。

- 只能在动态磁盘上创建跨区卷。
- 至少需要两个动态磁盘才能创建跨区卷。
- 跨区卷最多可以扩展到 32 个动态磁盘。
- 跨区卷无法镜像。
- 跨区卷不具备容错能力。

我们只能够使用 NTFS 文件系统来创建跨区卷。跨区卷不能是镜像卷并且不提供容错。如果包含一个跨区卷的磁盘出现故障，则整个卷将无法工作，且其上的数据都将丢失。

如果需要创建卷，但又没有足够的未分配空间分配给单个磁盘上的卷，则可通过将来自多个磁盘的未分配空间的扇区合并到一个跨区卷来创建足够大的卷。用于创建跨区卷的未分配空间区域的大小可以不同。跨区卷是这样组织的，先将一个磁盘上为卷分配的空间充满，然后从下一个磁盘开始，再将该磁盘上为卷分配的空间充满。跨区卷可以在不使用装入点的情况下获得更多磁盘上的数据。通过将多个磁盘使用的空间合并为一个跨区卷，从而可以释放驱动器号用于其他用途，并可创建一个较大的卷用于文件系统。

我们只能在动态磁盘上创建跨区卷，并且至少需要两个动态磁盘才能创建跨区卷。MS-DOS、Windows 95、Windows 98、Windows NT 4.0、Windows XP Home Edition 和其他缺乏动态存储功能的操作系统无法识别通过 Windows 2000、Windows XP Professional、Windows Server 2003 或 Windows Server 2008 家族操作系统创建的任何跨区卷。因此，如果创建双启动模式计算机上的带区卷，则其他操作系统将无法使用构成该卷的磁盘。

使用 NTFS 文件系统格式化的现有跨区卷可由所有磁盘上未分配空间的总量进行扩展。但是，在扩展跨区卷之后，不删除整个跨区卷将无法删除它的任何部分。Disk Management 可以格式化新的区域，但不会影响原跨区卷上现有的任何文件。

3. 带区卷(RAID - 0)

如图 11-32 所示，带区卷是通过将两个或更多动态磁盘上的可用空间区域合并到一个逻辑卷而创建的。带区卷使用 RAID-0，从而可以在多个磁盘上分布数据。带区卷不能被扩展或镜像，并且不提供容错。如果包含带区卷的其中一个磁盘出现故障，则整个卷无法工作。当创建带区卷时，最好使用相同大小、型号和制造商的磁盘。

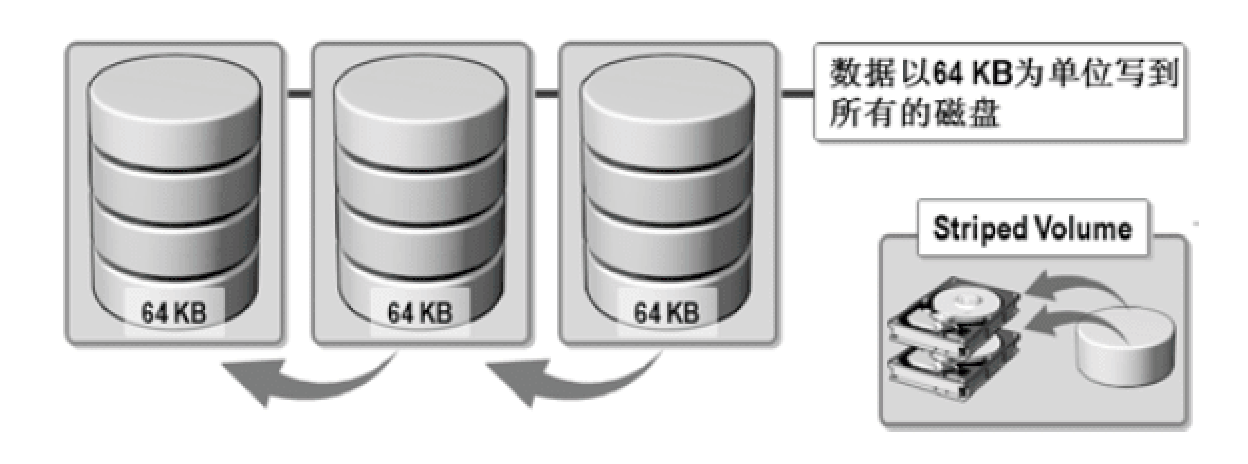


图 11-32　RAID-0

利用带区卷，可以将数据分块并按一定的顺序在阵列中的所有磁盘上分布数据，与跨区卷类似。带区卷可以同时对所有磁盘进行写数据操作，从而可以相同的速率向所有磁盘写数据。通过多个驱动器头可以访问分布在多个硬盘上的数据，来提高数据的读写性能。

尽管带区卷不具备容错能力，但带区卷在所有 Windows 磁盘管理策略中的性能最好，并且它通过同时在多个磁盘上分配 I/O 请求来提高 I/O 性能。

使用带区卷可以在下列情况提高 I/O 性能。

- 从(向)大的数据库中读(写)数据。
- 以极高的传输速率从外部源收集数据。
- 装载程序映像、动态链接库 (DLL) 或运行时库。

MS-DOS、Windows 95、Windows 98、Windows Millennium Edition、Windows NT 4.0、Windows XP Home Edition 和其他缺乏动态存储功能的操作系统无法识别通过 Windows 2000、Windows XP Professional、Windows Server 2003 或 Windows Server 2008 家族操作系统创建的任何带区卷。因此，如果创建双启动模式计算机上的带区卷，则其他操作系统将无法使用该卷。

4. 镜像卷(RAID -1)

如图 11-33 所示，镜像卷是具有容错能力的动态卷。它通过使用卷的两个副本或镜像复制存储在卷上的数据从而提供数据冗余性。写入到镜像卷上的所有数据都写入到位于独立的物理磁盘上的两个镜像中。

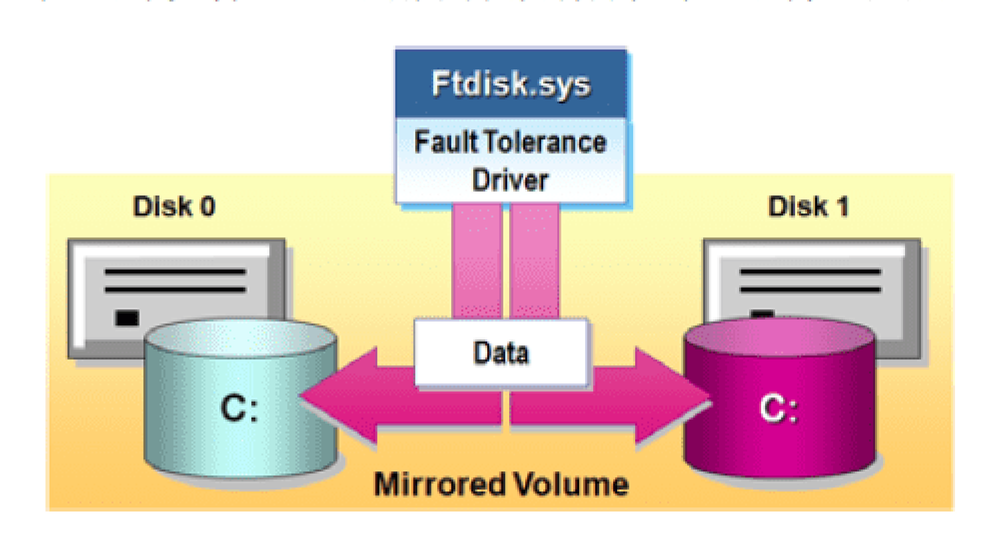


图 11-33　镜像卷(RAID-1)

如果其中一个物理磁盘出现故障，则该故障磁盘上的数据将不可用，但是系统可以使用未受影响的磁盘继续操作。当镜像卷中的一个镜像出现故障时，则必须将该镜像卷中断，使得另一个镜像成为具有独立驱动器号的卷；然后可以在其他磁盘中创建新镜像卷，该卷的可用空间应与之相同或更大。当创建镜像卷时，最好使用大小、型号和制造商都相同的磁盘。

由于双写入操作可能降低系统性能，所以许多镜像卷配置都是用双工模式。在这种模式中，镜像卷中的每个磁盘都有自己独立的磁盘控制器。双工镜像卷具有最佳的数据可靠性，因为复制了整个输入/输出(I/O) 子系统。这意味着如果某个磁盘控制器出现故障，其他控制器(及控制器上的磁盘)将继续正常运行。

如果没有使用双控制器，则出现故障的控制器将使镜像卷中的两份镜像不可访问，直到更换该控制器。

几乎任何卷都可以进行镜像，包括系统卷和启动卷。以后不能扩展镜像卷来增加其大小。在基于 Itanium 的计算机上，无法镜像 GUID 分区表 (GPT) 磁盘上的可扩展固件接口 (EFI) 系统分区。

镜像系统卷或启动卷时，可以对镜像卷中的各个磁盘使用单独的控制器，从而使系统配置具有更好的容错能力。这种方法使得系统可以经受住硬磁盘或磁盘控制器出故障的考验。当创建镜像卷时，最好使用大小、型号和制造商都相同的磁盘。如果使用双工技术，则推荐使用相同的磁盘和控制器，尤其是在计划镜像系统卷或启动卷时。

镜像系统卷时，始终测试以确保当某个磁盘出现故障时可从各个镜像启动操作系统。为防止出现启动问题，请始终使用同一磁盘和控制器。

镜像卷目前广泛应用在没有使用硬件 RAID 的简易服务系统中。

在两个物理磁盘上复制数据的容错卷。它通过使用卷的副本(镜像)复制该卷中的信息来提供数据冗余，镜像总位于另一个磁盘上。如果其中一个物理磁盘出现故障，则该故障磁盘上的数据将不可用，但是系统可以使用未受影响的磁盘继续操作。镜像卷可以看作硬件 RAID 中的 RAID1。

5. RAID-5 卷

如图 11-34 所示，具有数据和奇偶校验的容错卷，有时分布于三个或更多的物理磁盘，奇偶校验用于在阵列失效后重建数据。如果物理磁盘的某一部分失败，可以用余下的数据和奇偶校验信息重新创建磁盘上失败的那一部分上的数据。

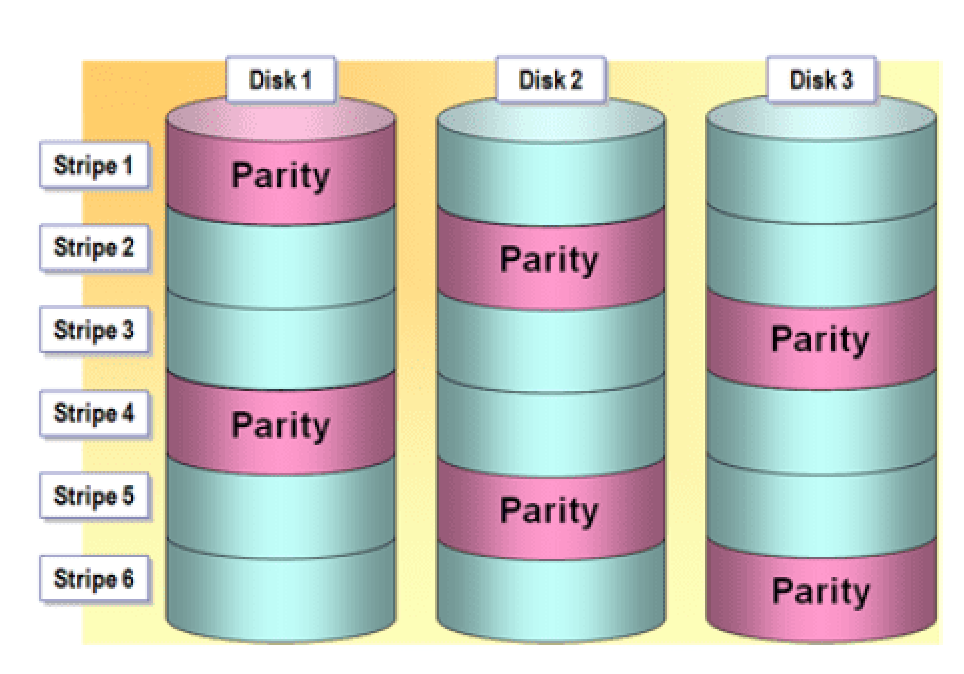


图 11-34　RAID-5 卷

RAID-5 可以理解为 RAID-0 和 RAID-1 的折衷方案。RAID-5 可以为系统提供数据安全保障，但保障程度要比 Mirror 低，而磁盘空间利用率要比 Mirror 高。RAID-5 具有和 RAID-0 相近似的数据读取速度，只是多了一个奇偶校验信息，写入数据的速度比对单个磁盘进行写入操作稍慢。同时由于多个数据对应一个奇偶校验信息，RAID-5 的磁盘空间利用率要比 RAID-1 高，存储成本相对较低。

11.5.2　简单卷管理

简单卷可以在不删除数据的情况下，增加空间或缩小空间。

示例 1：创建简单卷。

① 如图 11-35 所示，右击动态磁盘 1，从弹出的快捷菜单中选择“新建简单卷”命令。

② 如图 11-36 所示，在出现的“指定卷大小”对话框中，输入大小为 2000，单击“下一步”按钮。

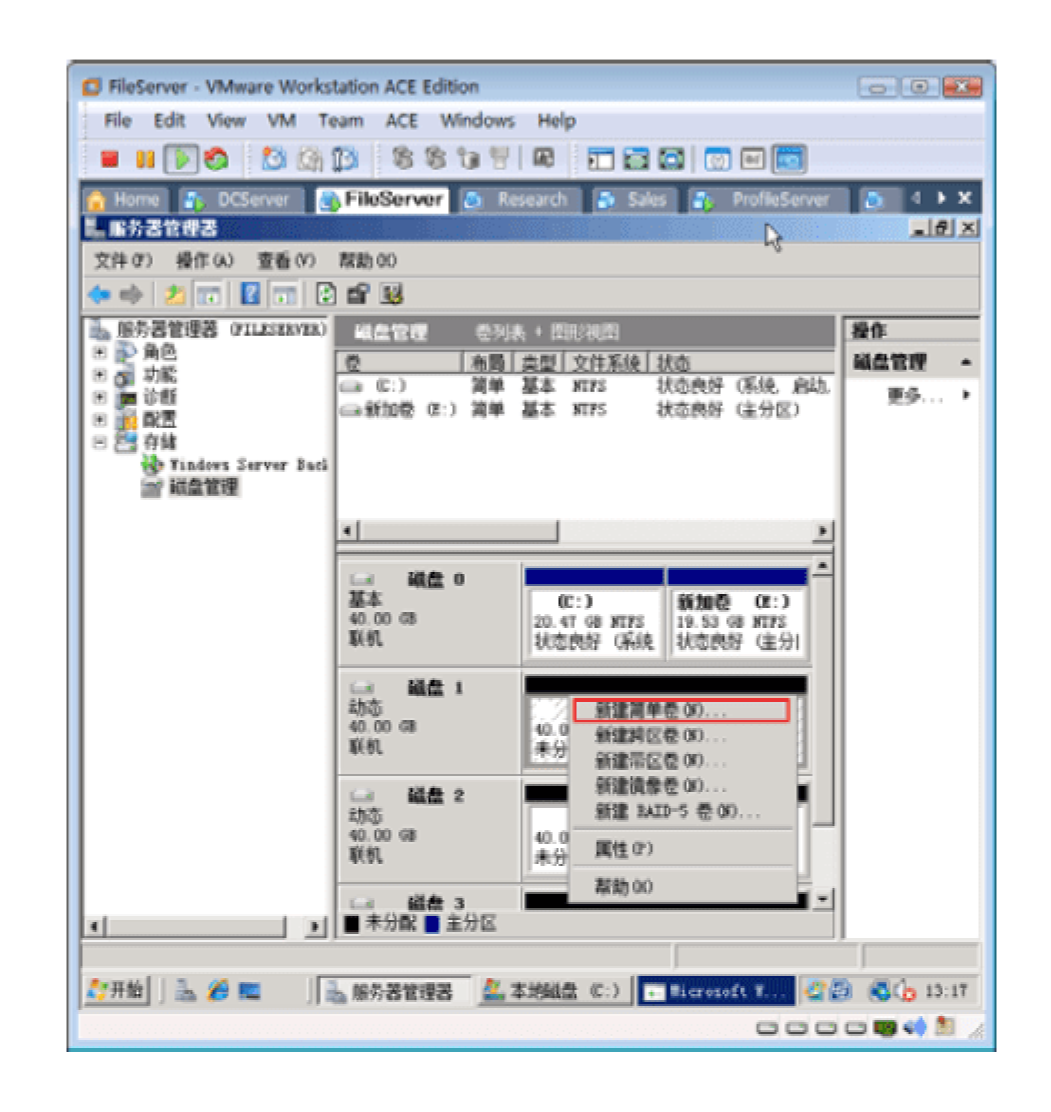


图 11-35 创建简单卷

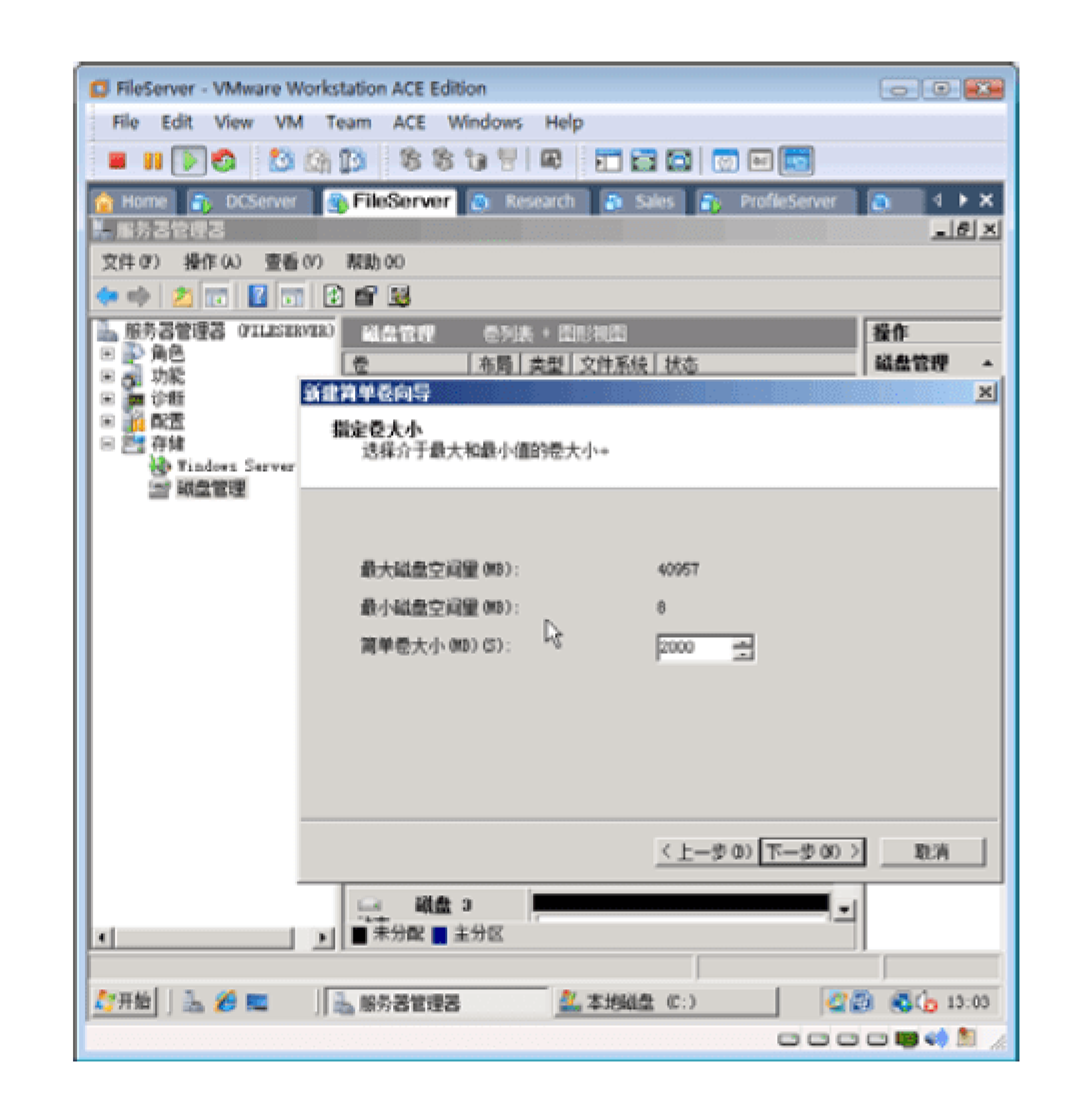


图 11-36 指定卷的大小

③ 如图 11-37 所示，在出现的“分配驱动器号和路径”界面中，指定盘符，单击“下一步”按钮。

④ 如图 11-38 所示，在出现的“格式化分区”界面中，选中“执行快速格式化”复选框，文件系统选中 NTFS，单击“下一步”按钮，完成简单卷的创建。

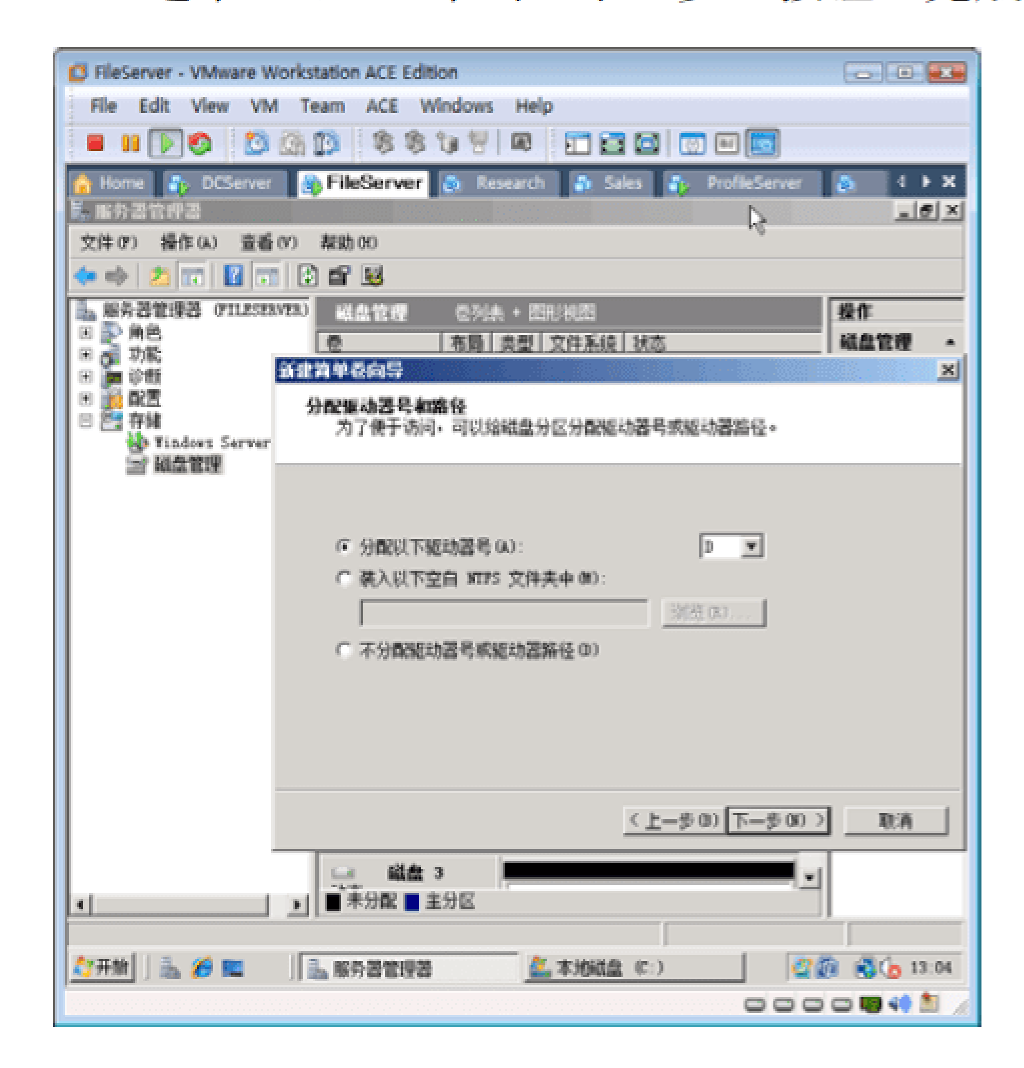


图 11-37 指定盘符

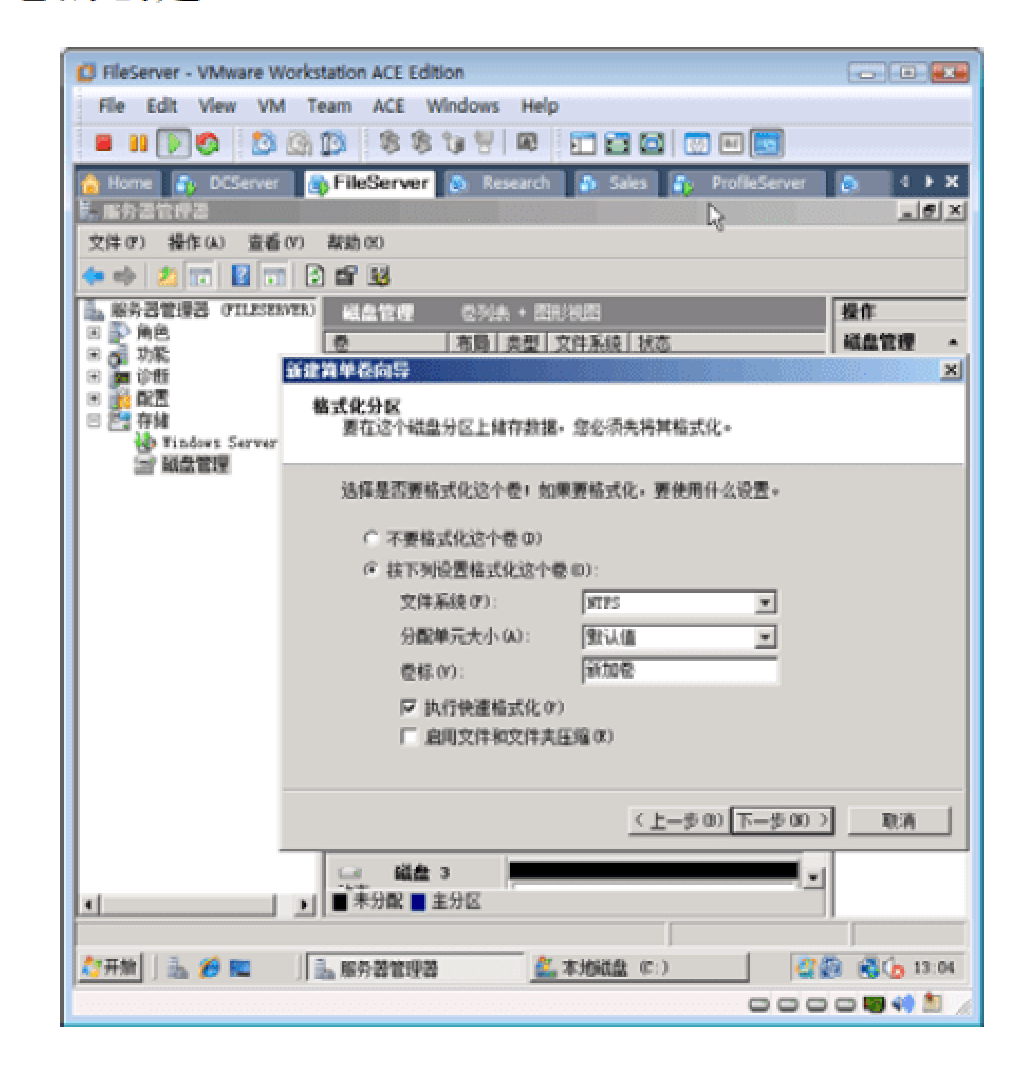


图 11-38 格式化硬盘

示例 2：扩展简单卷。

① 如图 11-39 所示，在创建 D 卷后又创建了 F 卷，后来发现动态磁盘上的简单卷 D 空间不够用了，这时可以扩展其空间。简单卷的空间可以不连续。

② 如图 11-40 所示，右击 D 卷，在弹出的快捷菜单中选择“扩展卷”命令。

③ 如图 11-41 所示，在出现的“选择磁盘”界面中输入扩展的大小，单击“下一步”按钮。

④ 如图 11-42 所示，可以看到 D 卷的空间可以不连续，中间有 F 卷。

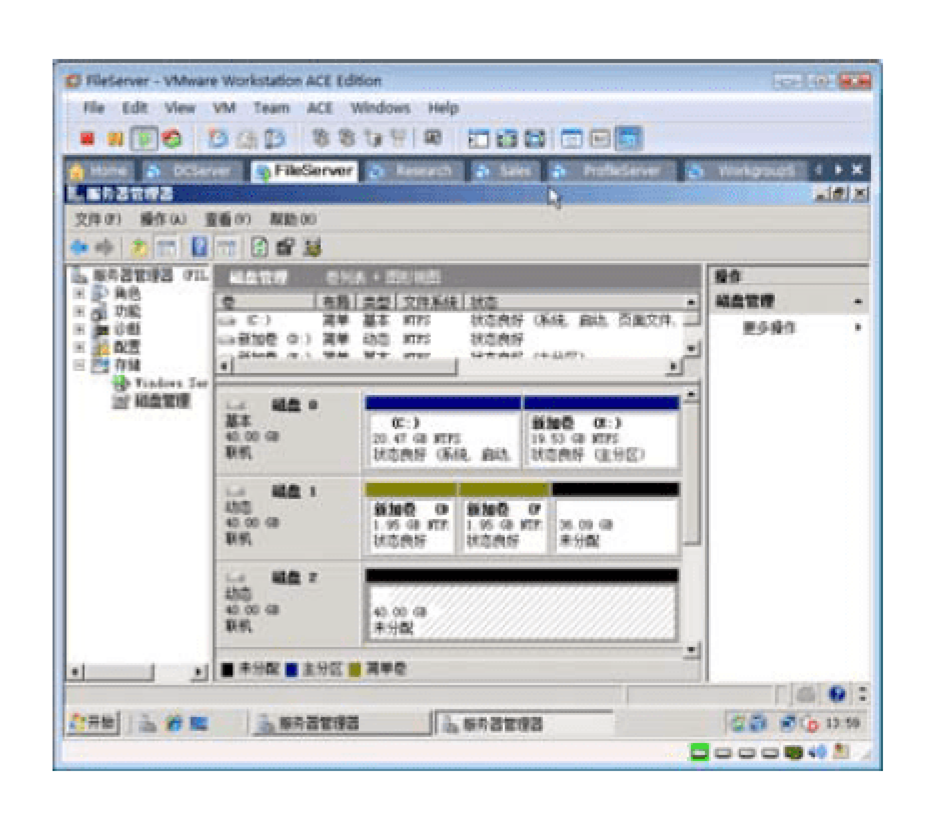


图 11-39　扩展卷(一)

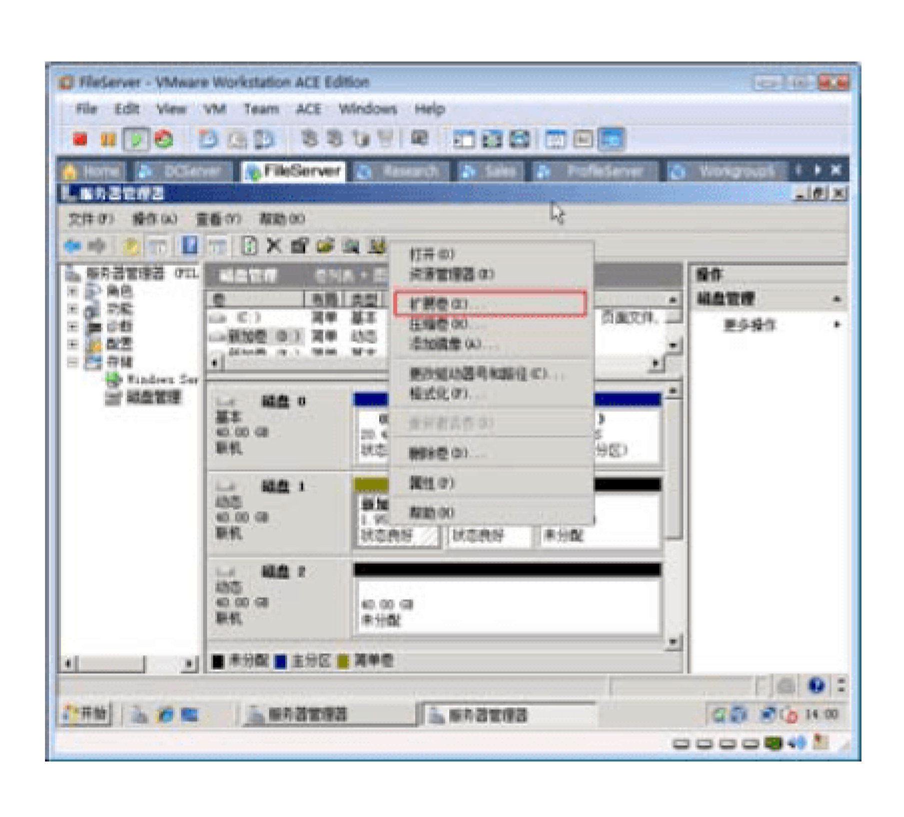


图 11-40　扩展卷(二)

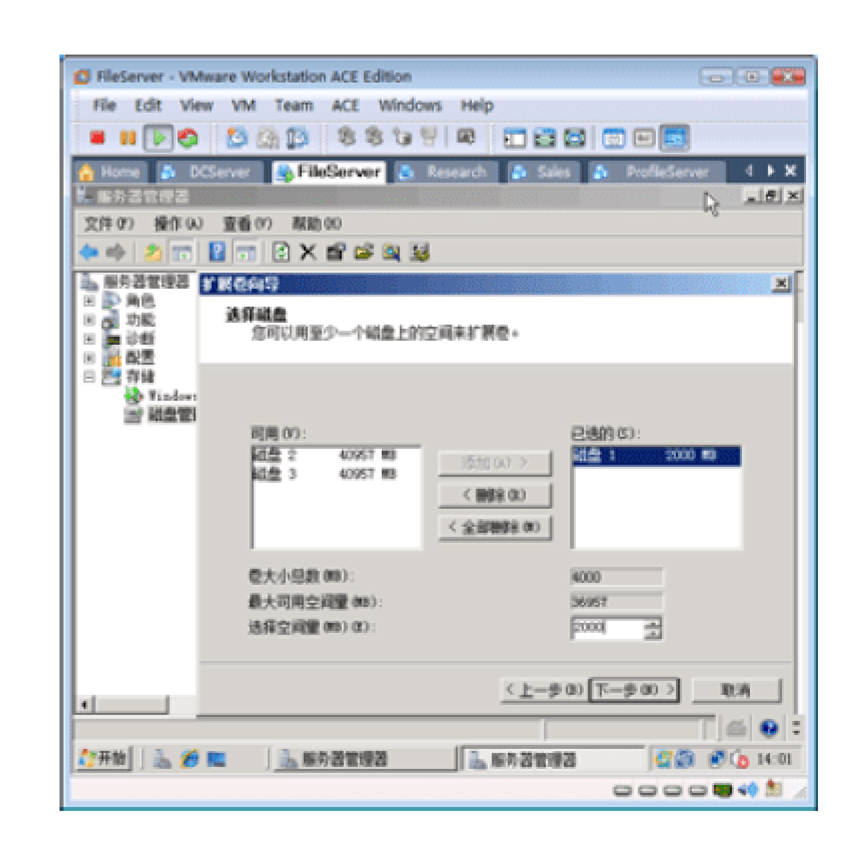


图 11-41　选定磁盘指定大小

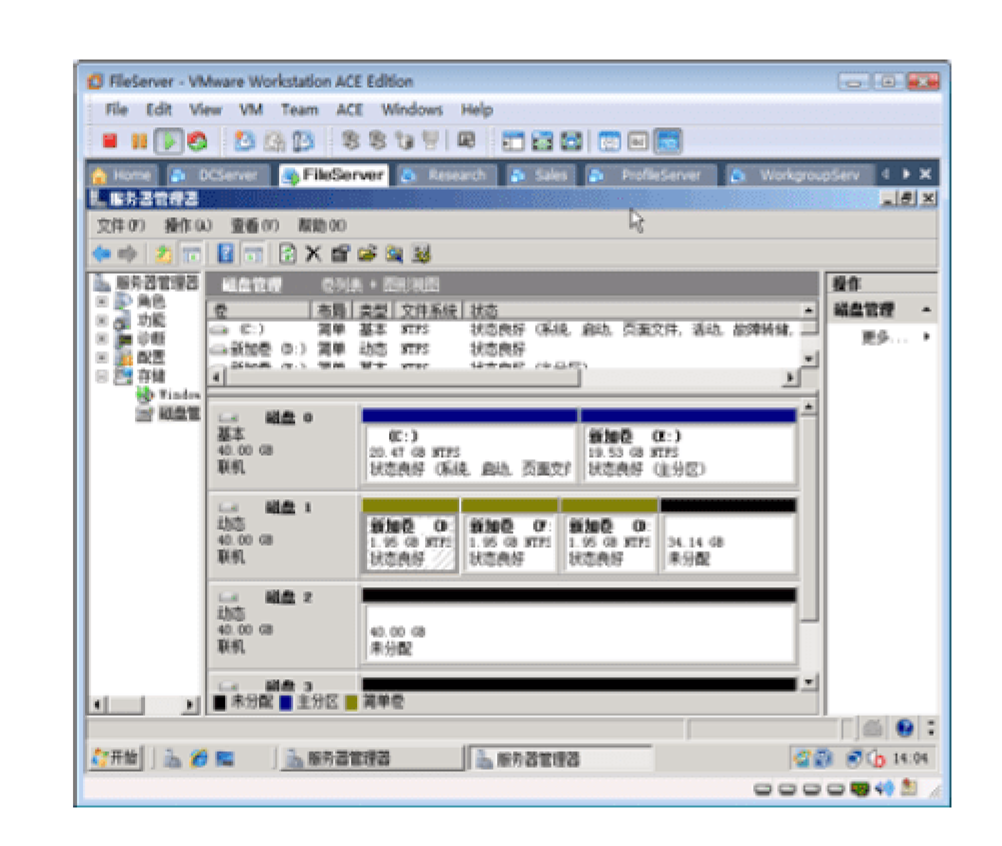


图 11-42　卷可以不连续

示例 3：收缩卷。

如果卷的空间太大，可以收缩。

① 如图 11-43 所示，右击 D 卷，从弹出的快捷菜单中选择“压缩卷”命令。

② 如图 11-44 所示，输入减少空间的大小，单击“压缩”按钮。

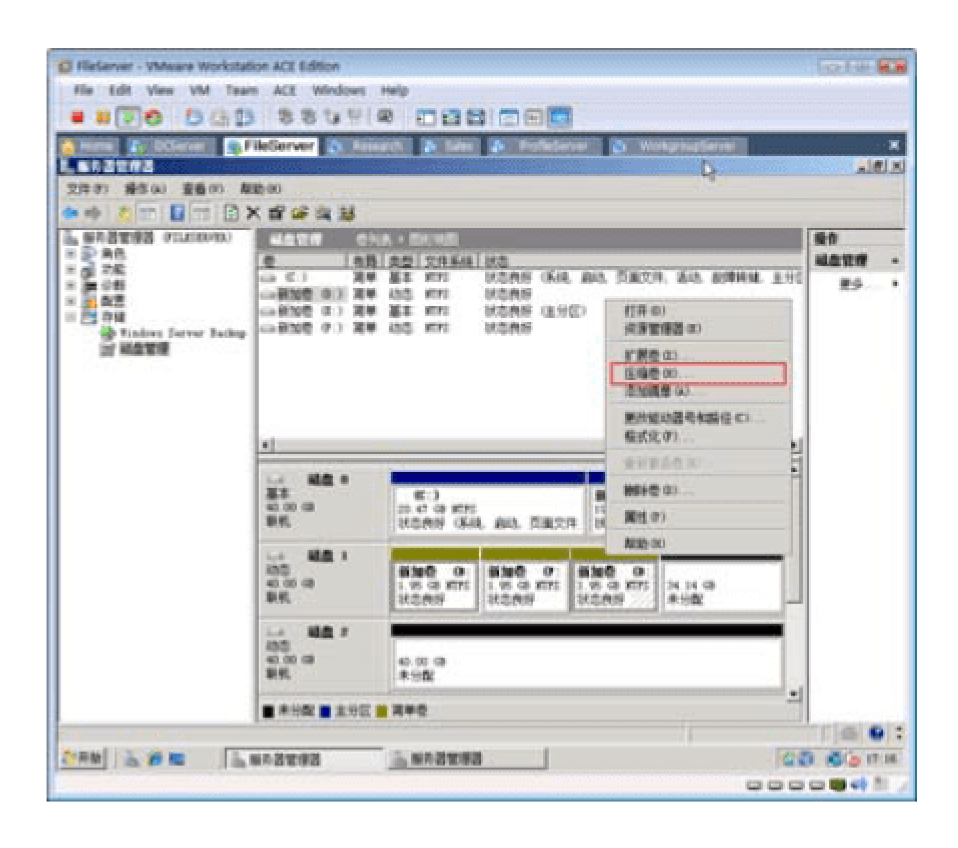


图 11-43　压缩卷

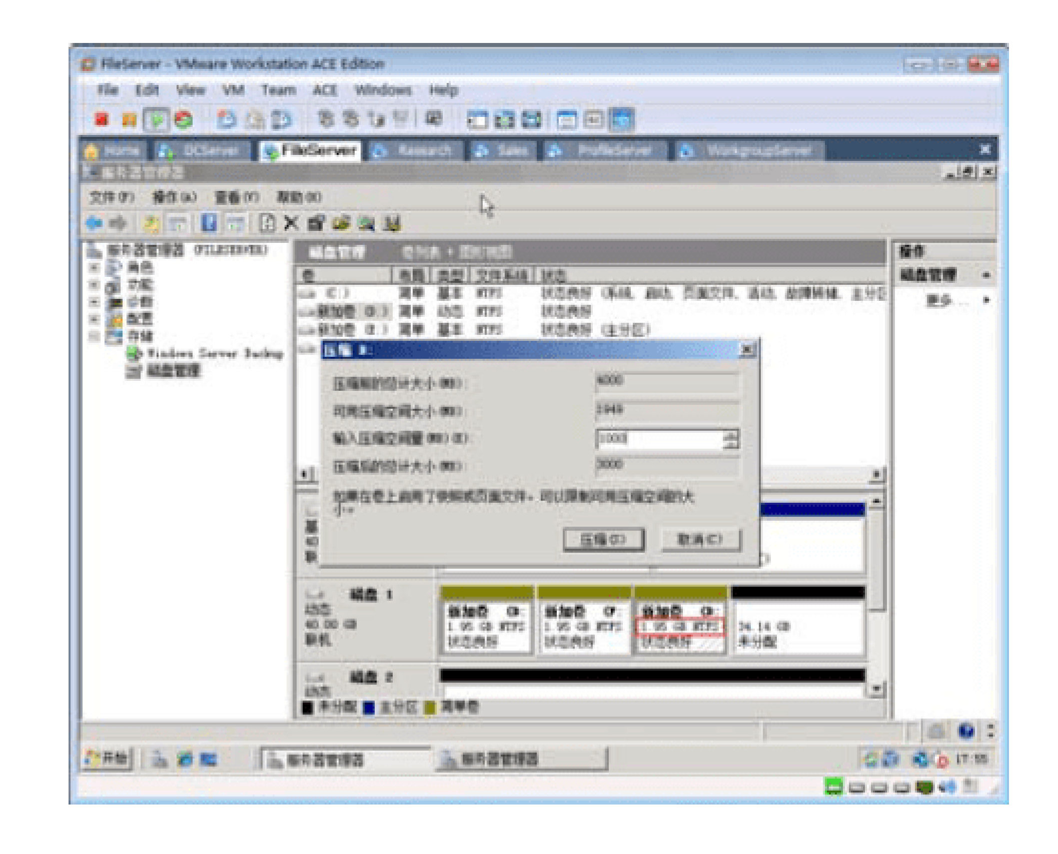


图 11-44　输入减少空间大小

③ 如图 11-45 所示，可以看到扩展出来的 D 卷右侧部分已经变为 1000 MB 大小。

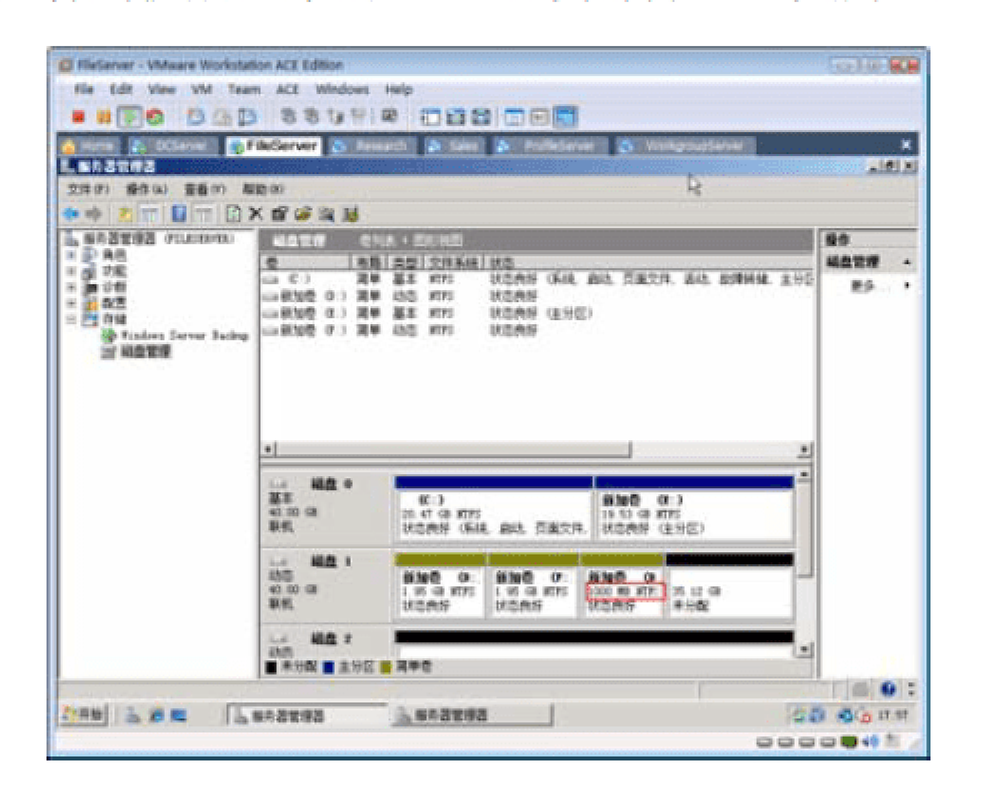


图 11-45 压缩后的大小

示例 4：添加镜像。

简单卷可以添加镜像，和另外一块硬盘的空间形成镜像关系，这样就可以实现容错了。

① 如图 11-46 所示，右击 D 卷，从弹出的快捷菜单中选择“添加镜像”命令。

② 如图 11-47 所示，在出现的“添加镜像”对话框中，选中磁盘 2，单击“添加镜像”按钮。

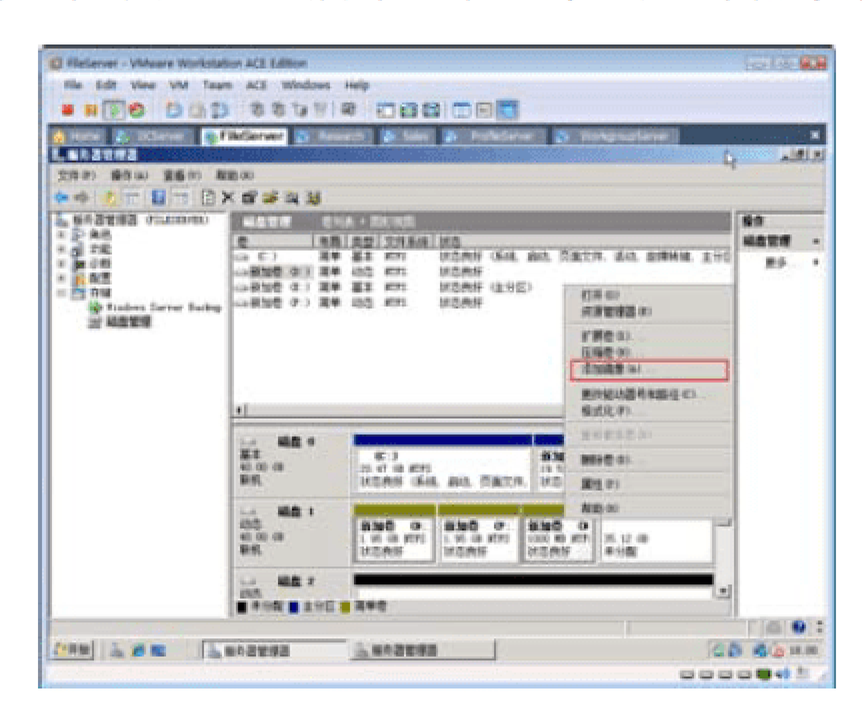


图 11-46 添加镜像

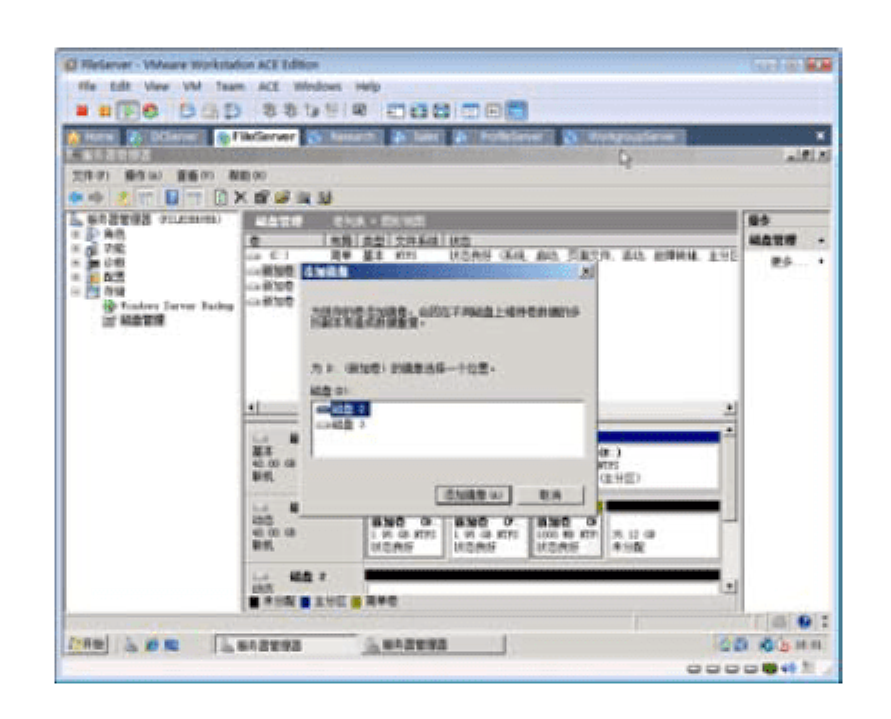


图 11-47 选择磁盘

③ 如图 11-48 所示，可以看到磁盘 2 上分出和 D 卷一样大小的空间作为镜像。

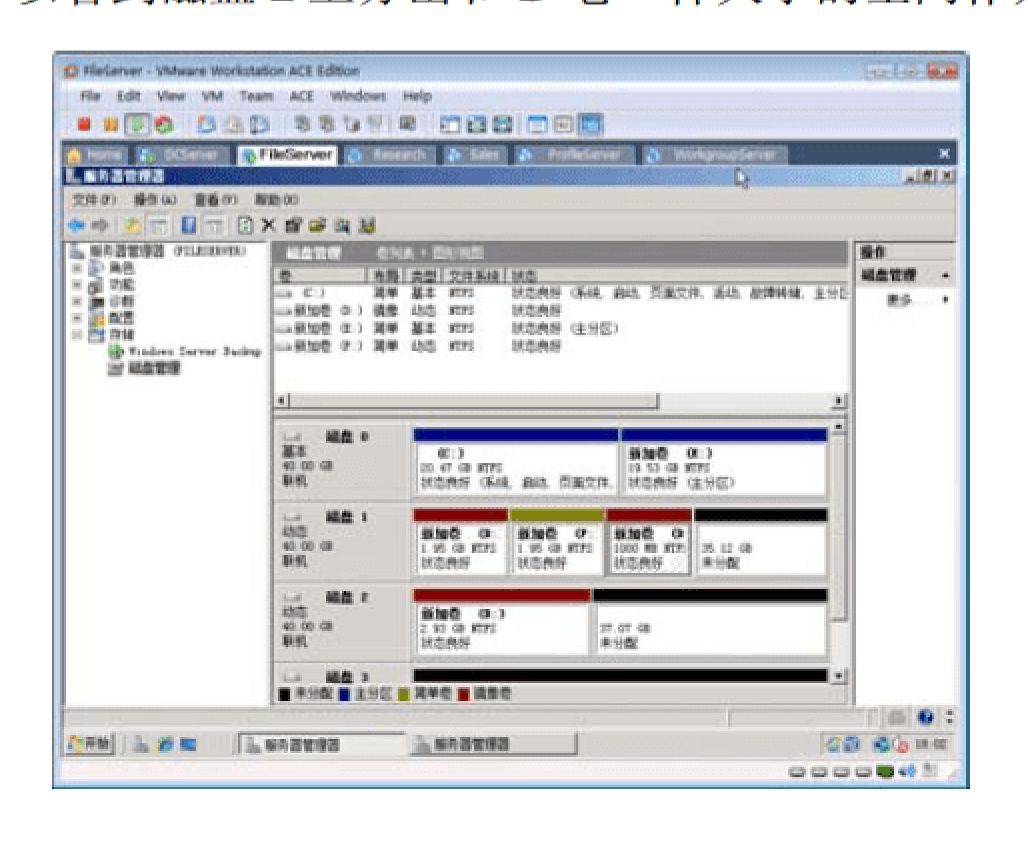


图 11-48 简单卷转成镜像卷

11.5.3　镜像卷管理

示例 1：新建镜像卷。

① 如图 11-49 所示，右击动态磁盘磁盘 1，从弹出的快捷菜单中选择“新建镜像卷”命令。

② 如图 11-50 所示，在出现的“新建镜像卷”对话框中选中磁盘 2，单击“添加”按钮，输入磁盘空间大小，可以看到两个磁盘各拿出 2000 MB，但卷的大小是 2000 MB，单击“下一步”按钮。

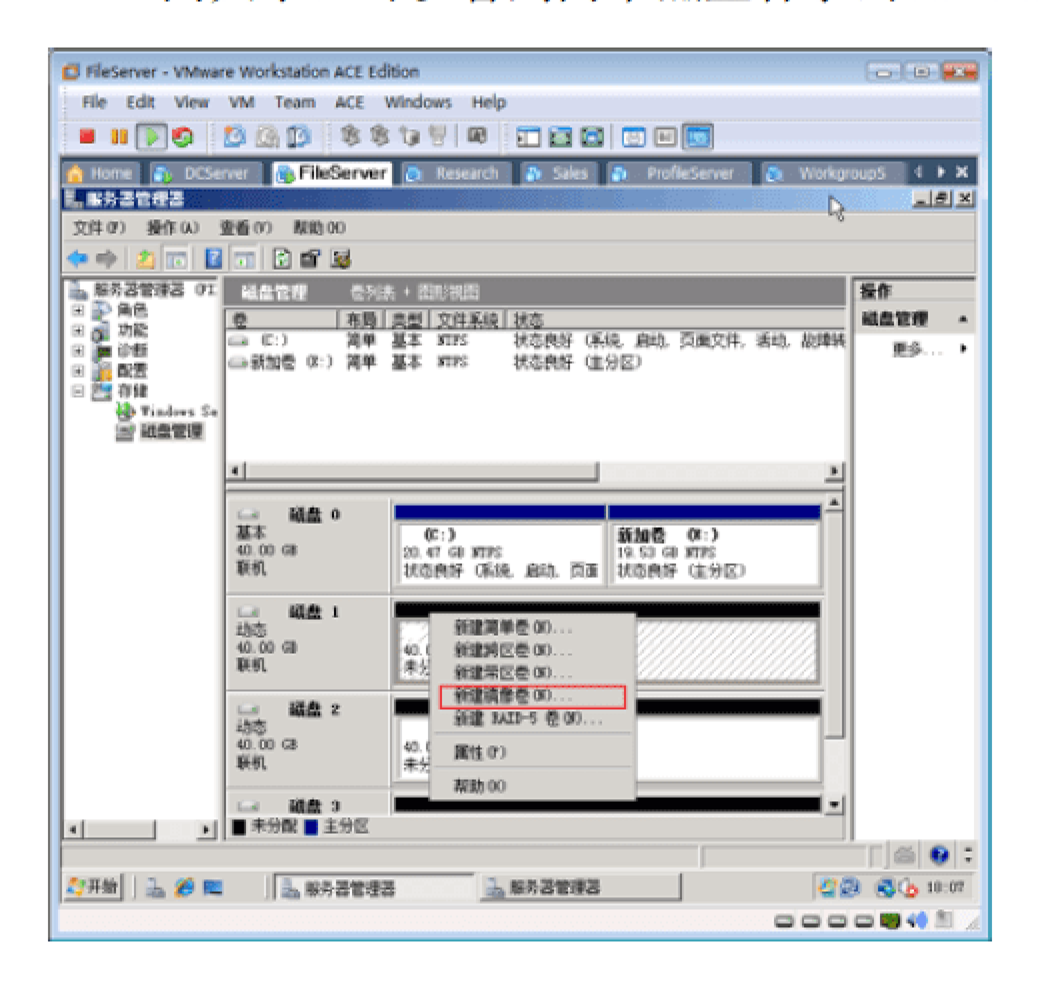


图 11-49　创建镜像卷

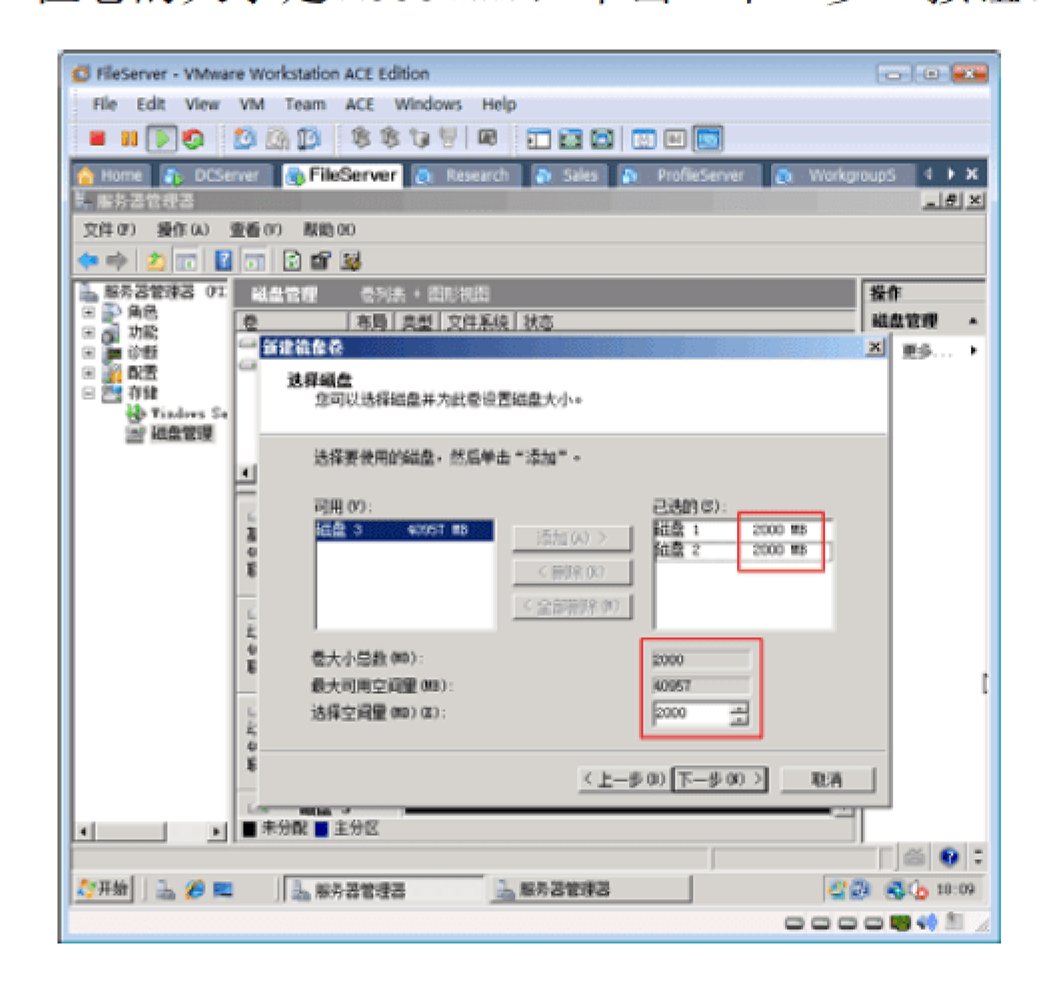


图 11-50　指定磁盘和卷大小

③ 如图 11-51 所示，在出现的“分配驱动器号和路径”界面中指定盘符，单击“下一步”按钮。

④ 如图 11-52 所示，在出现的“卷区格式化”界面中选中“执行快速格式化”复选框，单击“下一步”按钮，完成创建。

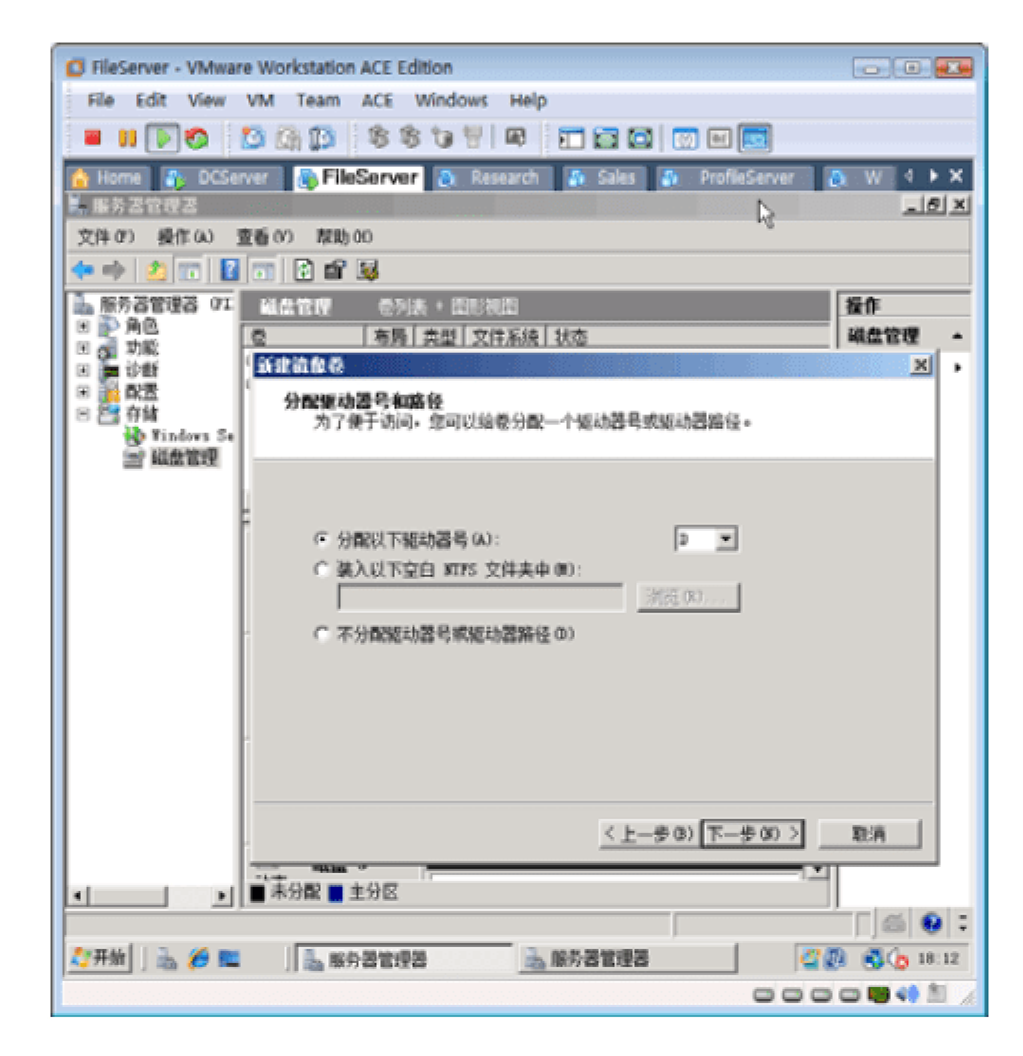


图 11-51　分配盘符和路径

图 11-52　卷区格式化

⑤ 如图 11-53 所示，可以看到新建的镜像卷。

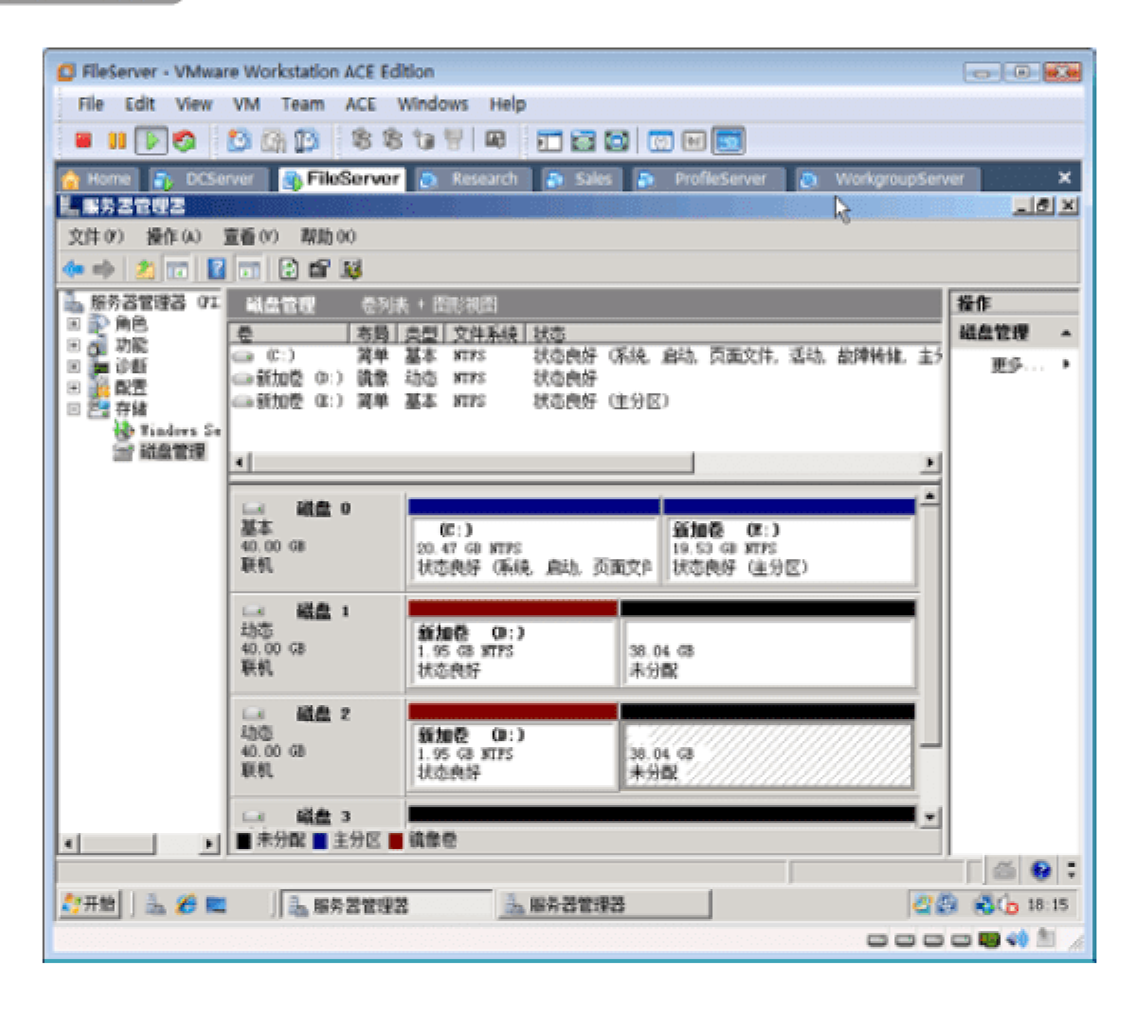


图 11-53 镜像卷

示例 2：中断镜像卷。

中断镜像卷，可以将镜像卷变成两个简单卷，失去容错。

① 如图 11-54 所示，右击镜像卷，从弹出的快捷菜单中选择“中断镜像卷”命令，在出现的对话框中单击“是”按钮。

② 如图 11-55 所示，可以看到出现了两个简单卷。

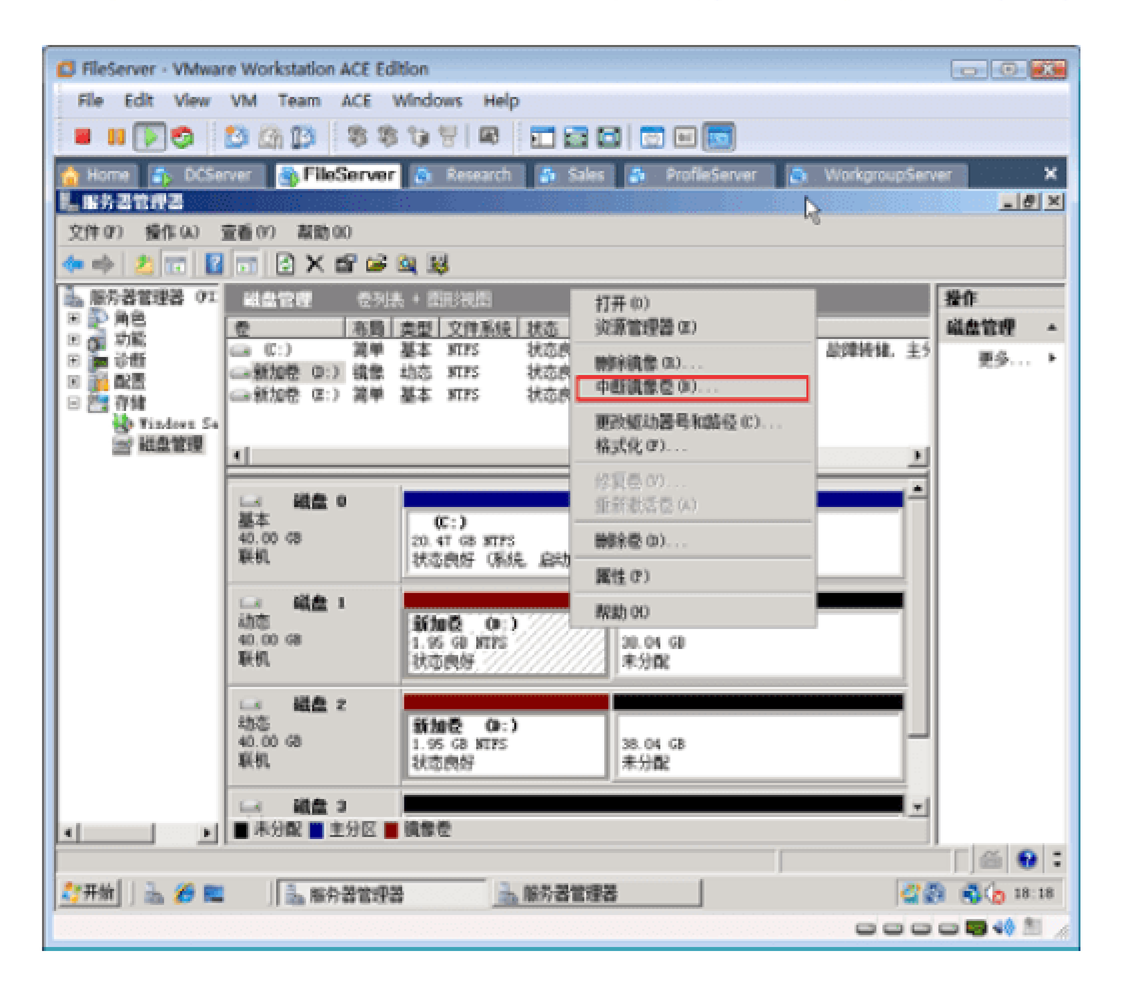


图 11-54 中断镜像

图 11-55 变成两个简单卷

示例 3：删除镜像卷。

可以删除磁盘 2 上的镜像，这样就会将镜像卷变成一个简单卷。

① 如图 11-56 所示，右击镜像卷，从弹出的快捷菜单中选择“删除镜像”命令。

② 如图 11-57 所示，选中要删除镜像卷的磁盘，单击“删除镜像”按钮。在出现的提示对话框中单击“是”按钮。

③ 如图 11-58 所示，可以看到，只留下磁盘 1 上的卷，已经变为简单卷。

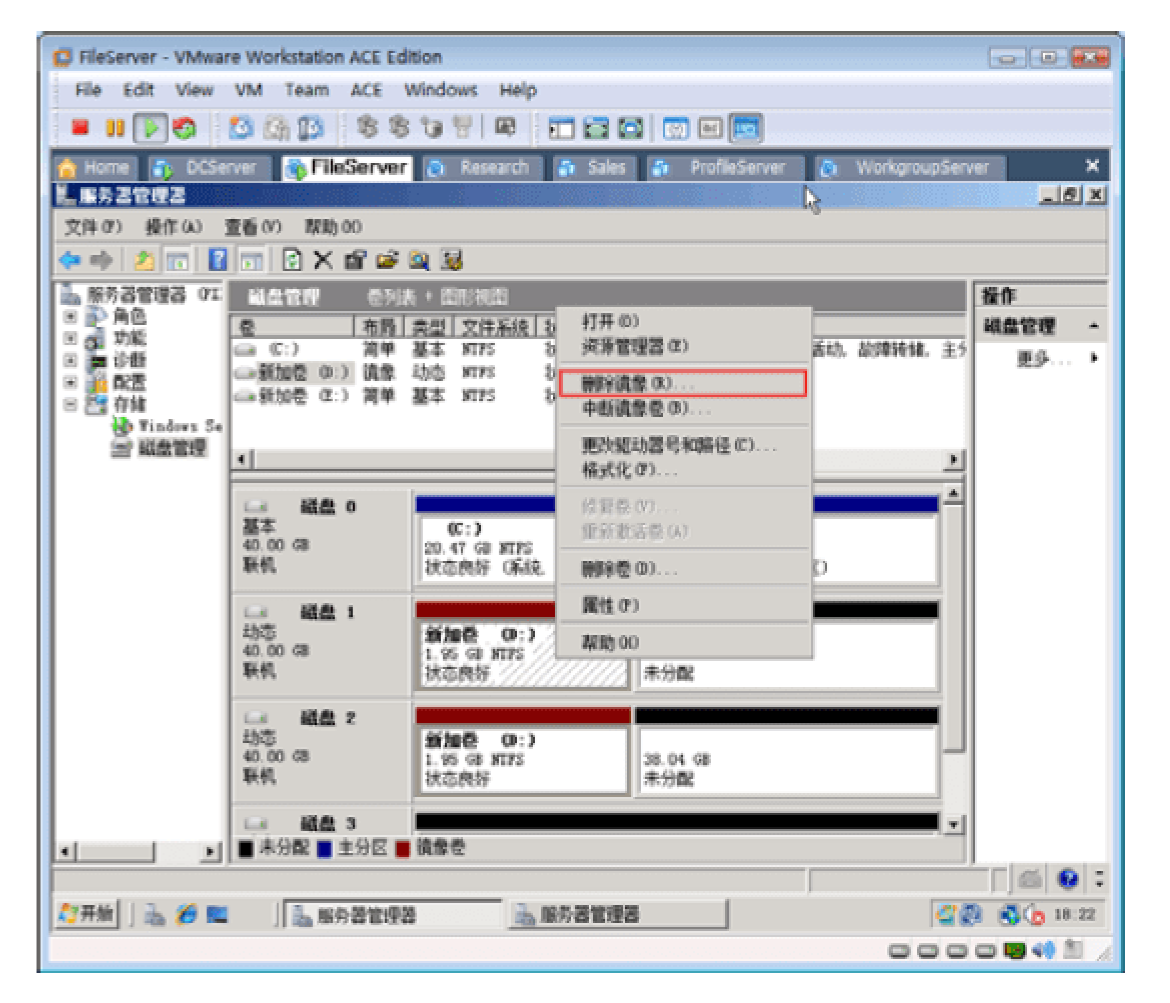


图 11-56　删除镜像(一)

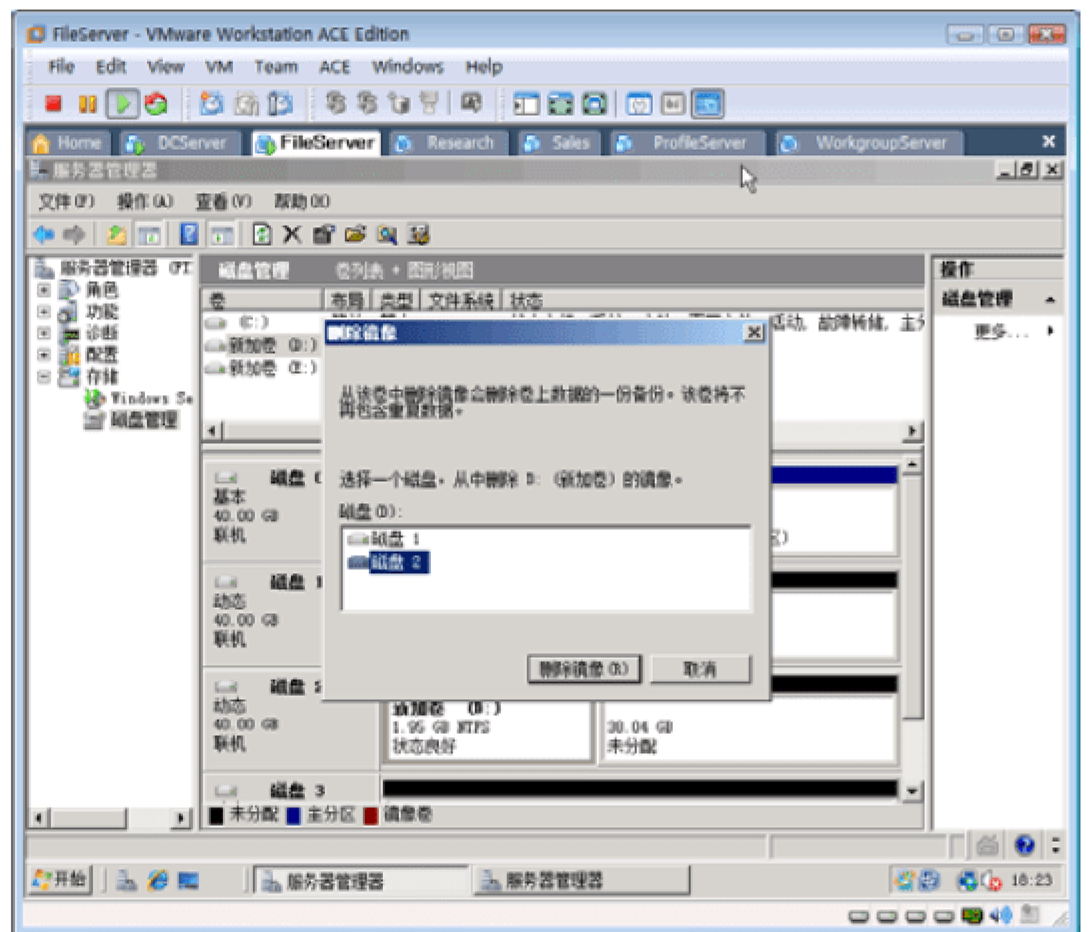


图 11-57　删除镜像(二)

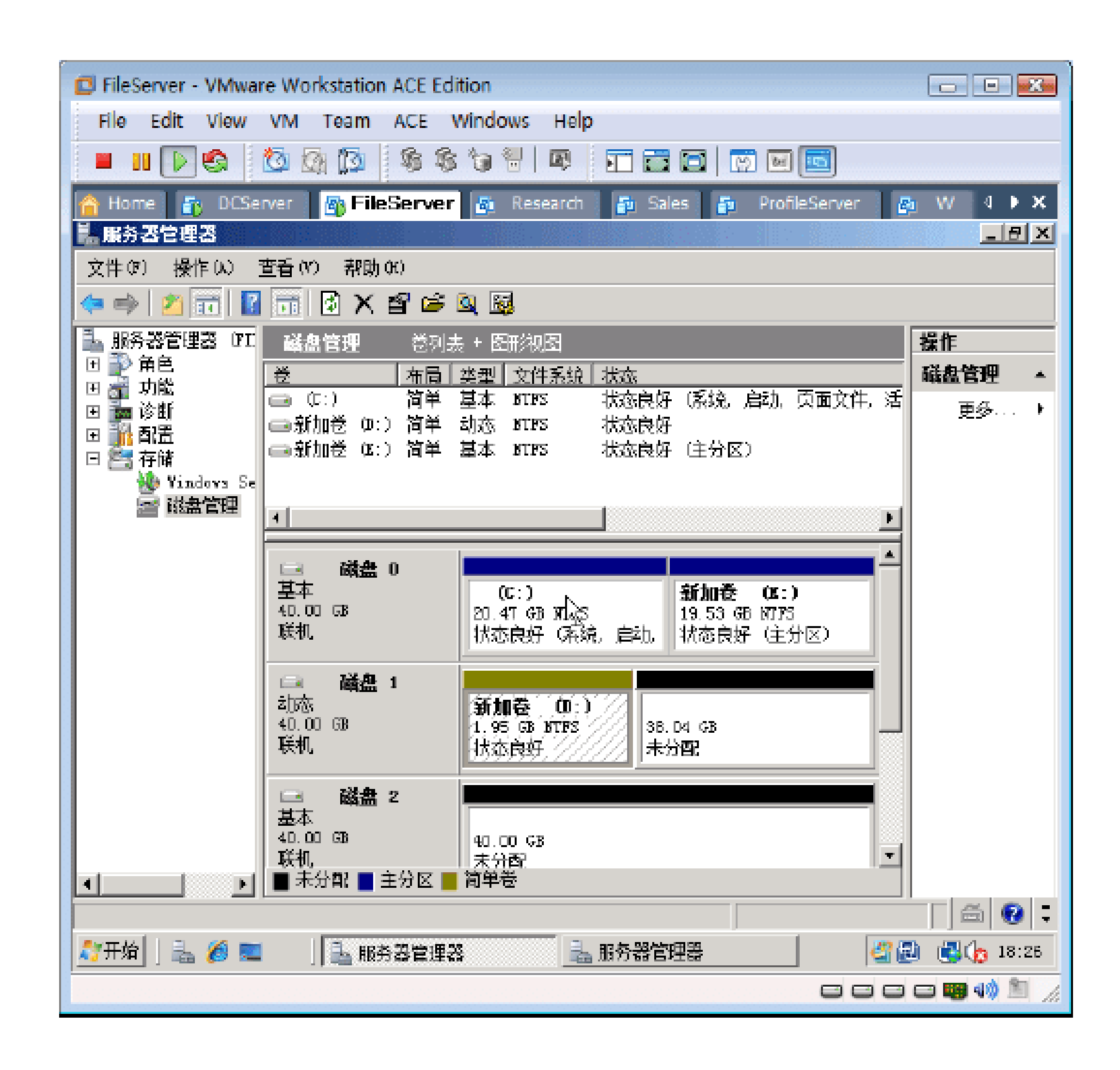


图 11-58　镜像卷变简单卷

11.5.4　RAID -5 管理

示例：创建 RAID-5 卷。

① 如图 11-59 所示，右击动态磁盘，从弹出的快捷菜单中选择“新建 RAID-5 卷”命令。

② 如图 11-60 所示，在出现的“选择磁盘”界面中，单击“添加”按钮，添加 3 个磁盘，输入磁盘大小，单击“下一步”按钮。

③ 如图 11-61 所示，在出现的“分配驱动器号和路径”界面中，选择驱动器号，单击“下一步”按钮。

④ 如图 11-62 所示，在出现的“卷区格式化”界面中，选中“执行快速格式化”复选框，单击“下一步”按钮。

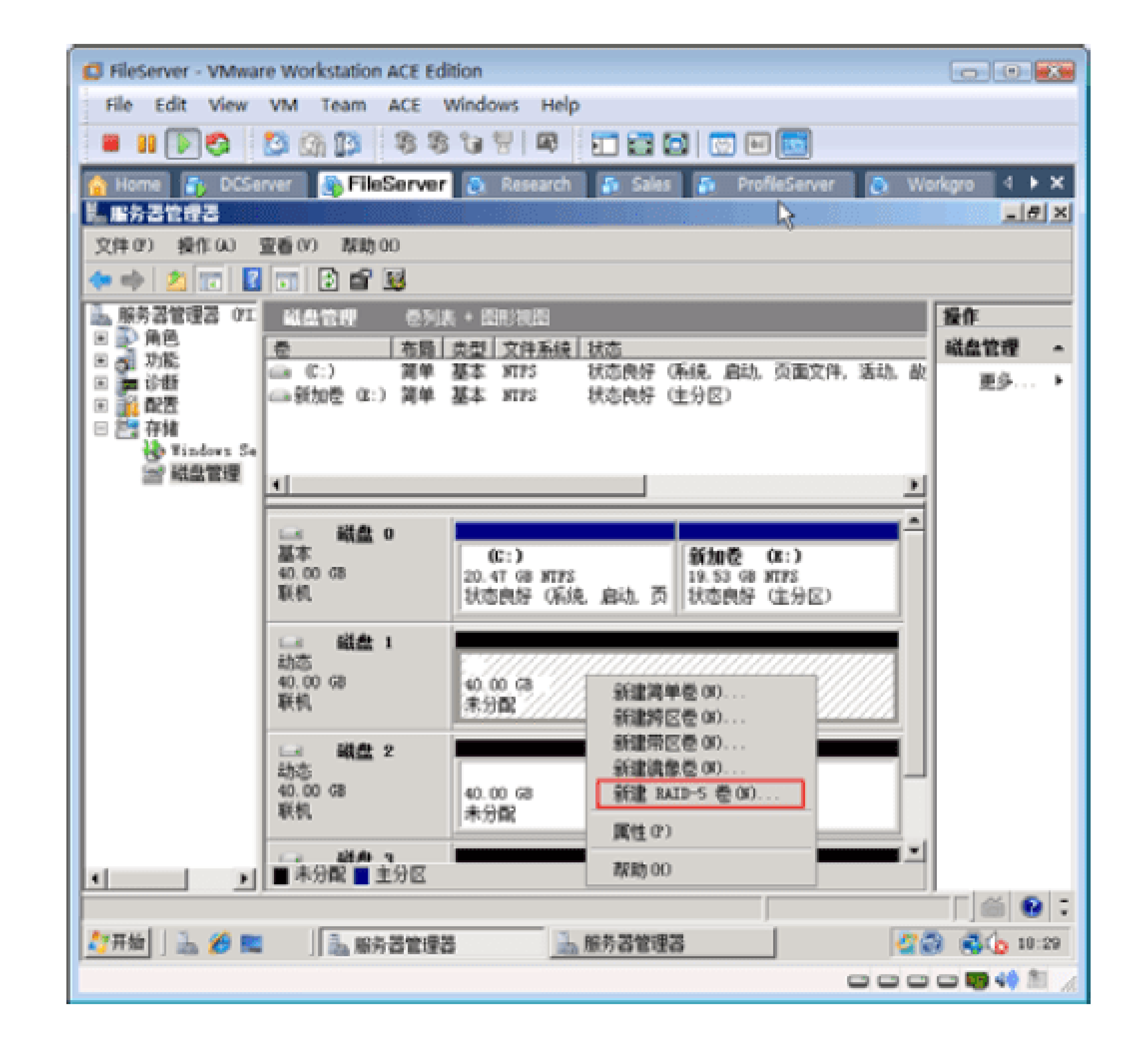


图 11-59 创建 RAID-5 卷

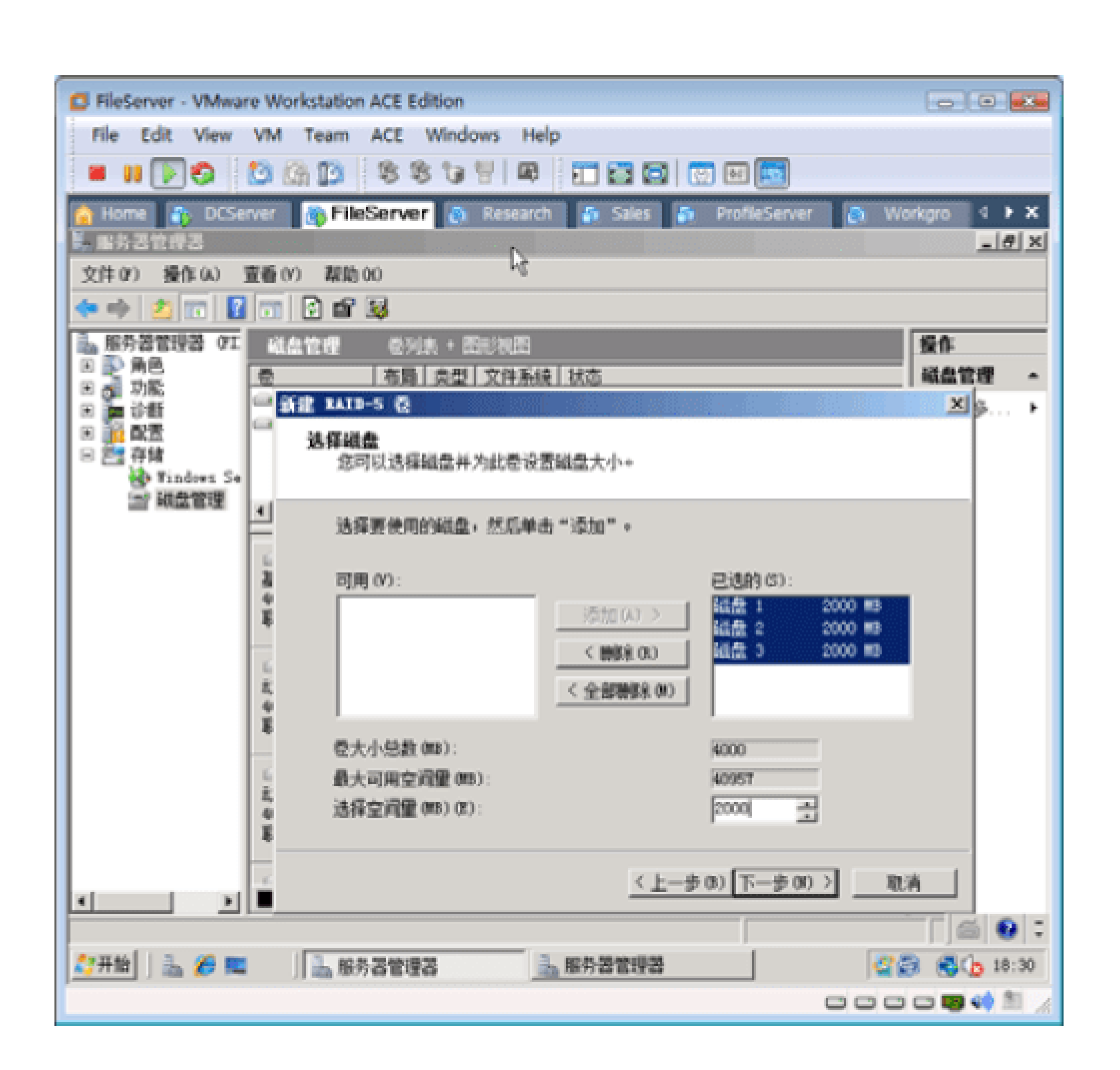


图 11-60 选择磁盘

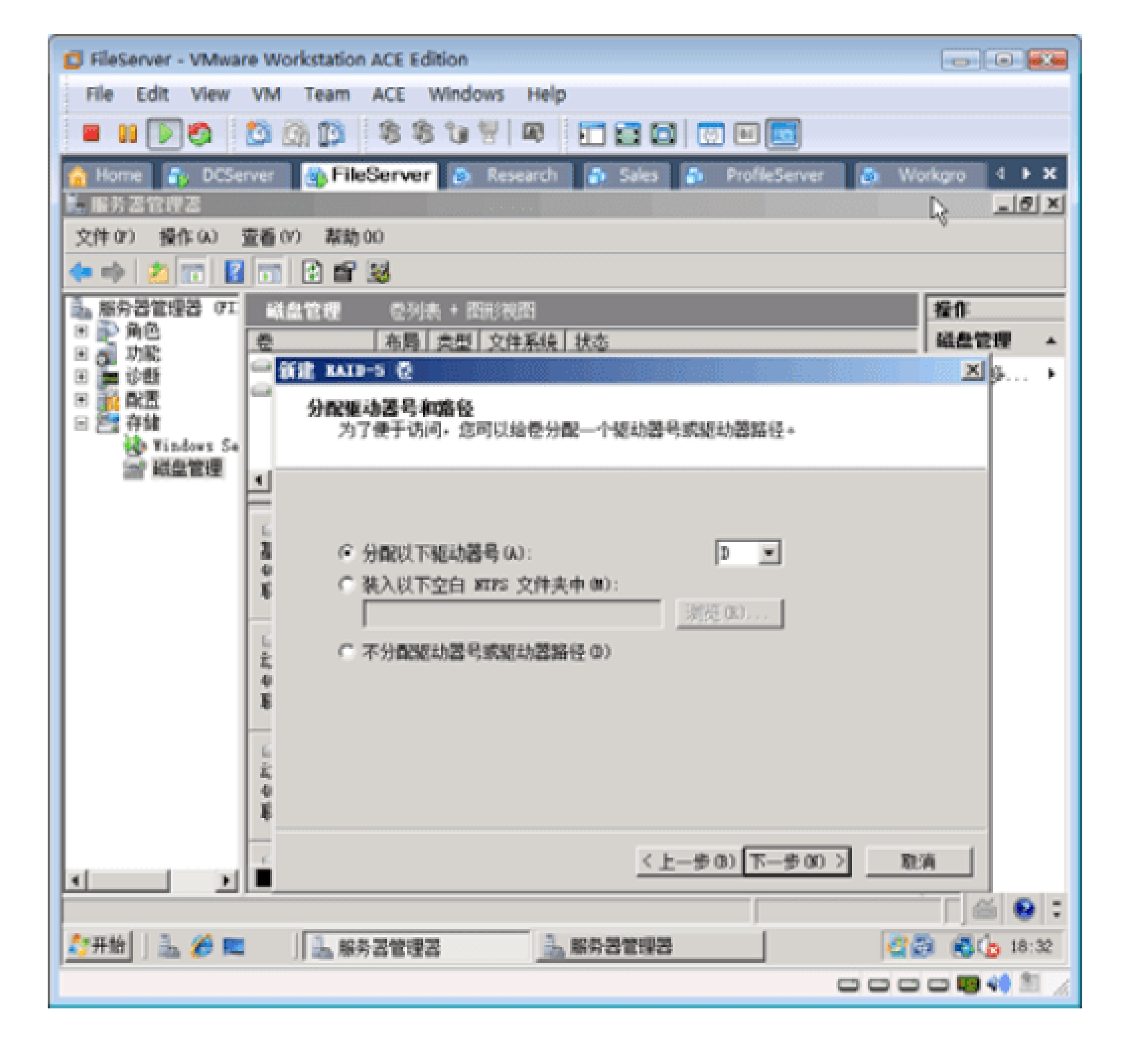


图 11-61 指定盘符

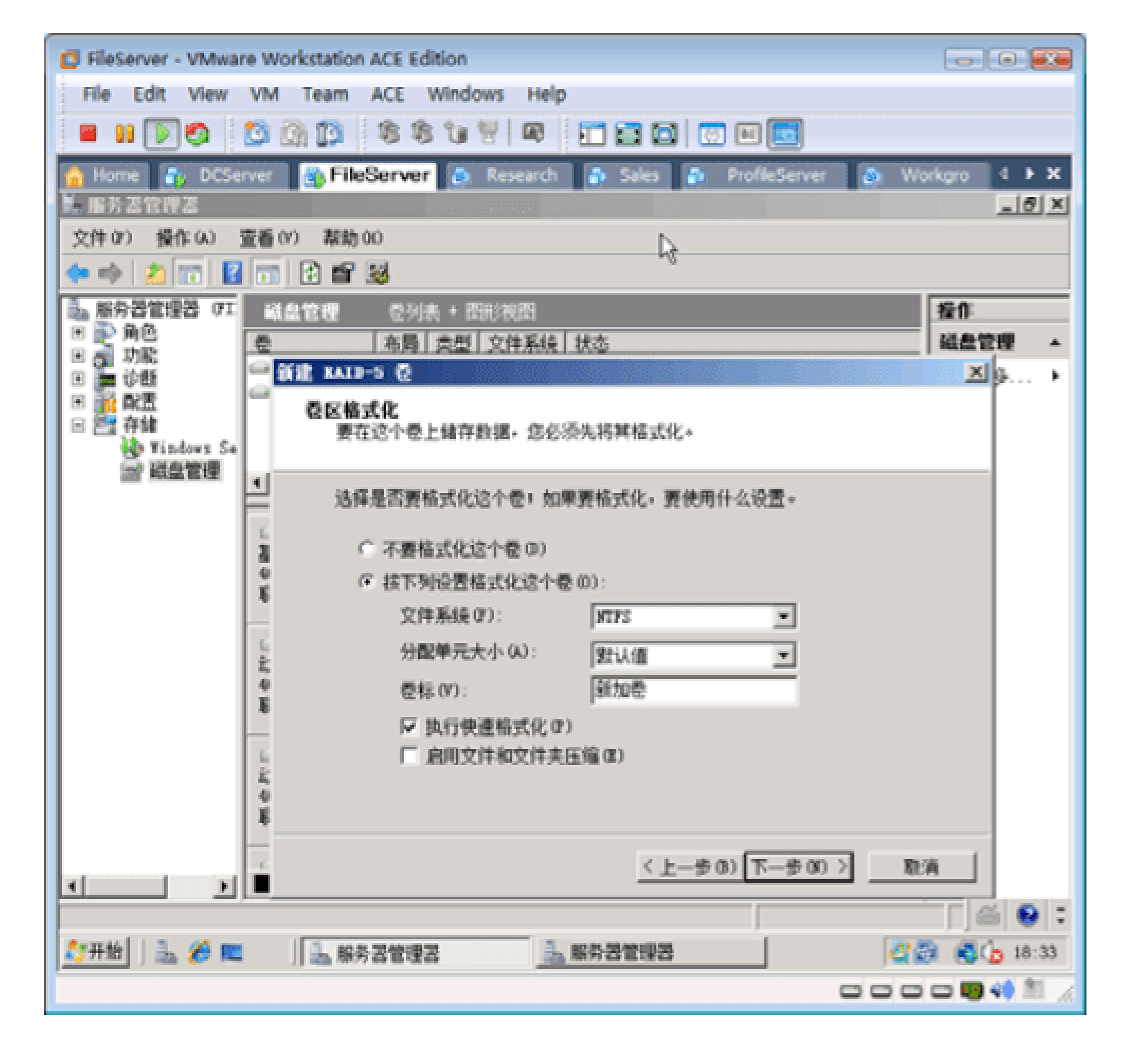


图 11-62 快速格式化

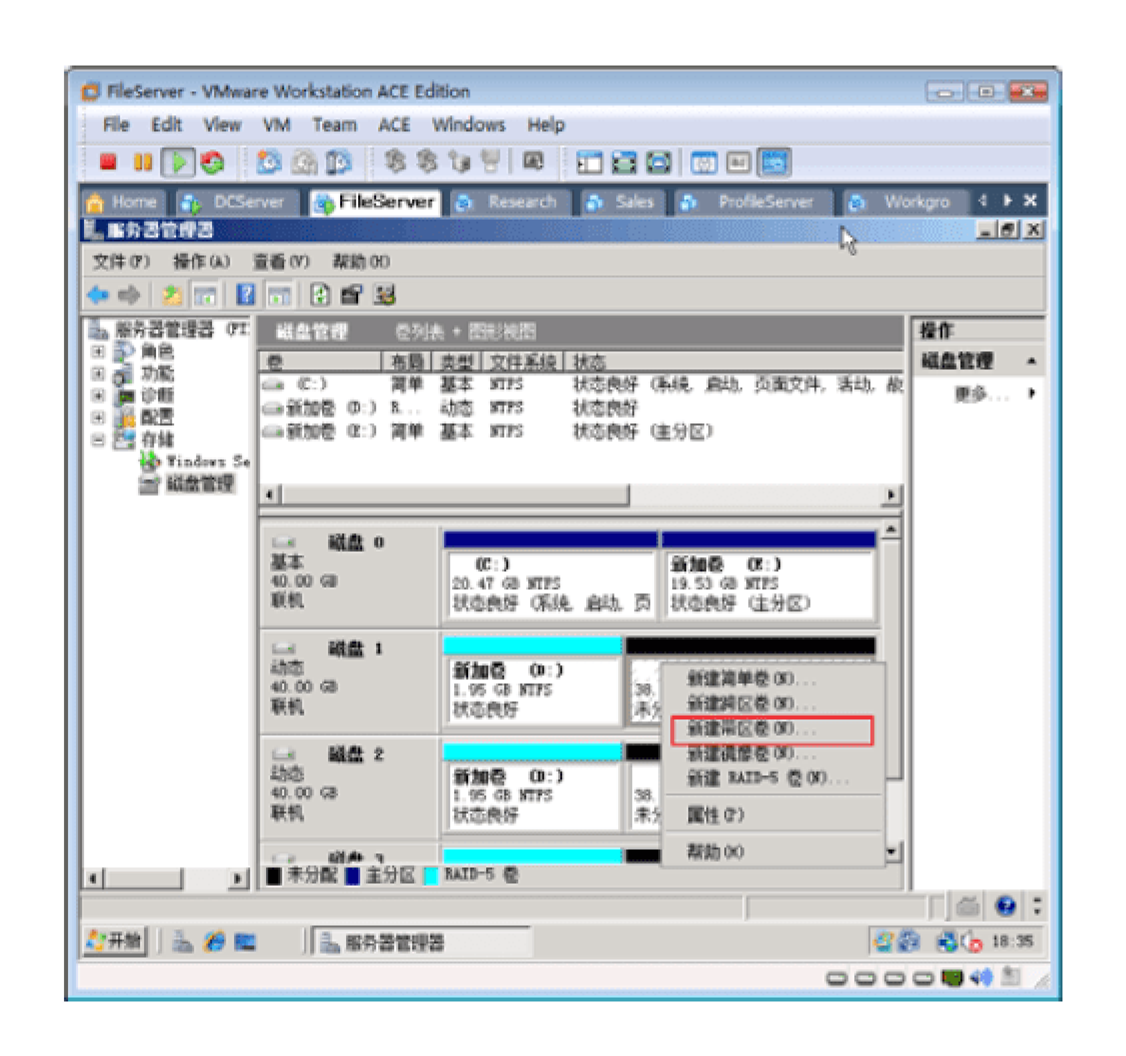
11.5.5 带区卷管理

示例：创建带区卷。

① 如图 11-63 所示，右击动态磁盘未分配空间，从弹出的快捷菜单中选择“新建带区卷”命令。

② 如图 11-64 所示，在“选择磁盘”界面中添加 3 块硬盘，输入大小 2000，可以看到整个卷的大小为 6000 MB。单击“下一步”按钮。

③ 指定驱动器号，选中“快速格式化”复选框，单击“下一步”按钮，完成带区卷创建。



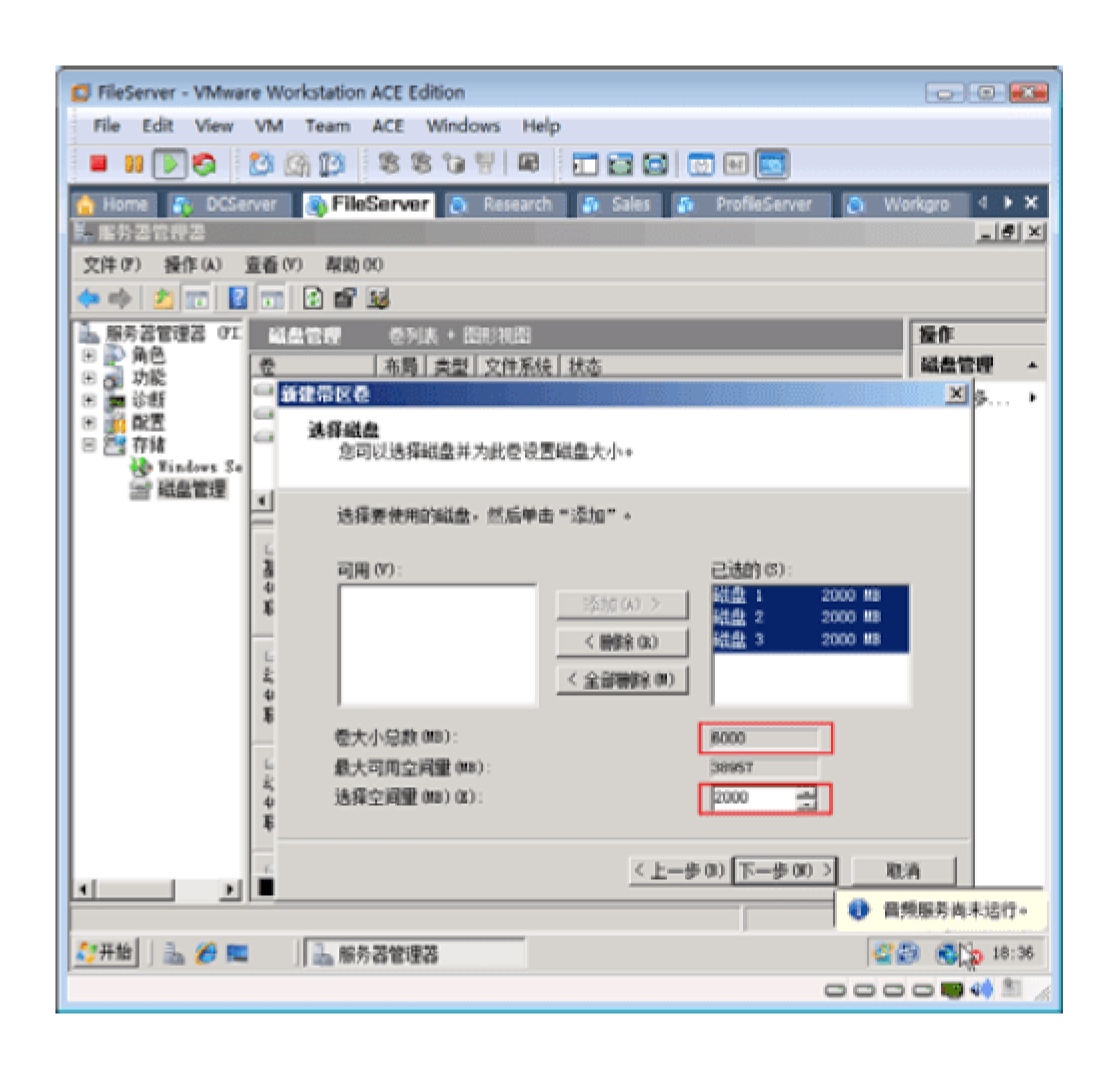




图 11-63　创建带区卷

图 11-64　选择磁盘并指定大小

11.5.6　跨区卷管理

示例：创建跨区卷。

① 如图 11-65 所示，右击动态磁盘未分配空间，从弹出的快捷菜单中选择“新建跨区卷”命令。

② 如图 11-66 所示，单击添加磁盘 1、磁盘 2、磁盘 3。指定使用每个磁盘的空间，单击“下一步”按钮。

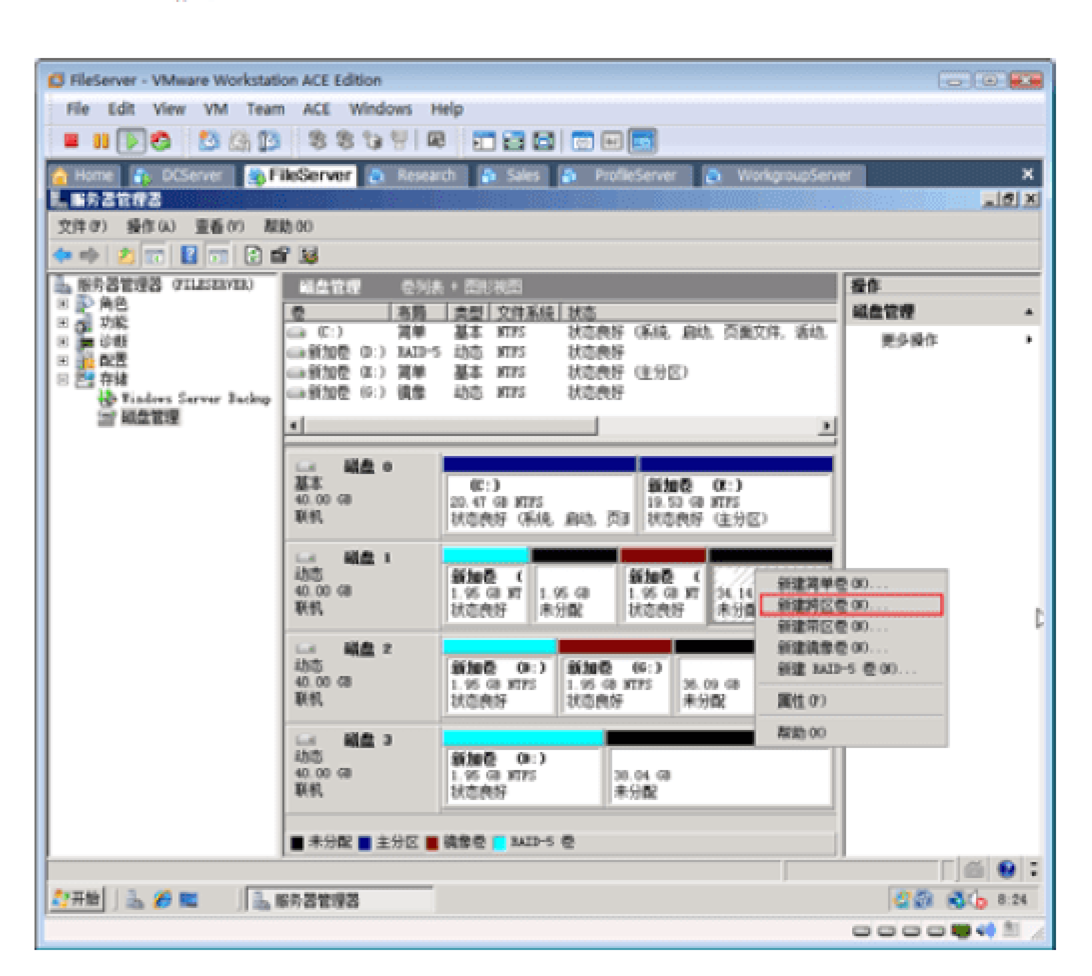


图 11-65　创建跨区卷

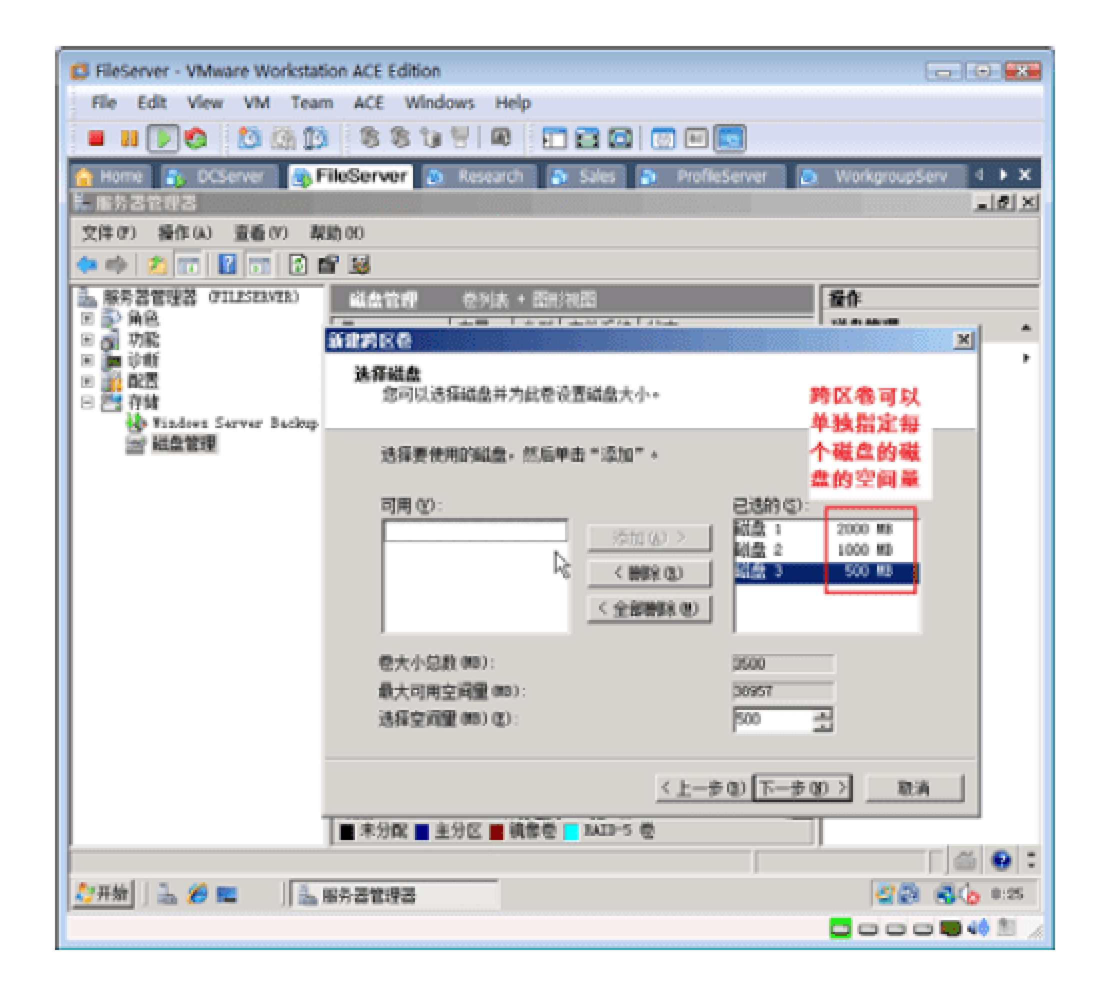


图 11-66　选择磁盘和指定大小

③ 指定驱动器号，选中“快速格式化”复选框，单击“下一步”按钮。如图 11-67 所示，F 卷是创建好的跨区卷。

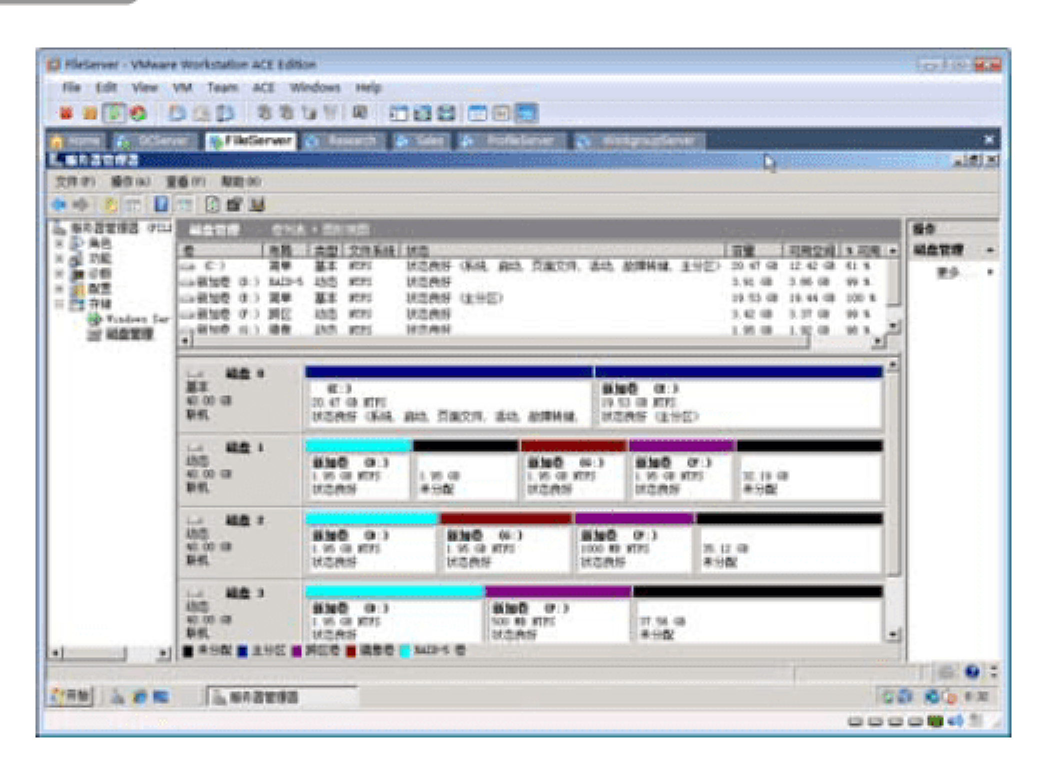


图 11-67　创建的跨区卷

11.5.7　使用卷的原则

使用卷应遵循如下几个原则。

- 如果存放的数据非常重要，但数据量不是很大，应创建镜像卷存储。比如一些财务报表、销售数据、客户资料等。
- 如果存放的数据非常重要，且数据量很大，为了充分利用磁盘空间，并且还要有冗余，应创建 RAID-5 卷存储，比如数据库文件。
- 如果存储的数据不是很重要，并且有备份，为了获得较好的读写性能，应创建带区卷存储，比如流媒体服务器上的视频文件。
- 为了将多个动态磁盘的零散的磁盘空间整合成一个较大的卷，应创建跨区卷。

11.6　动态磁盘灾难恢复

以下试验将会演示磁盘 2 坏掉后，添加一块新的磁盘 newDisk，然后修复 RAID-5 和镜像卷。并能够看到带区卷已经没有办法修复。

如图 11-68 所示，创建 RAID-5 卷 D 卷，带区卷 F 卷，镜像卷 G 卷。使用的磁盘空间如图 11-68 所示。通过在各个卷创建文件来验证坏掉磁盘 2 后，哪些卷还能够访问，且文件不丢失。

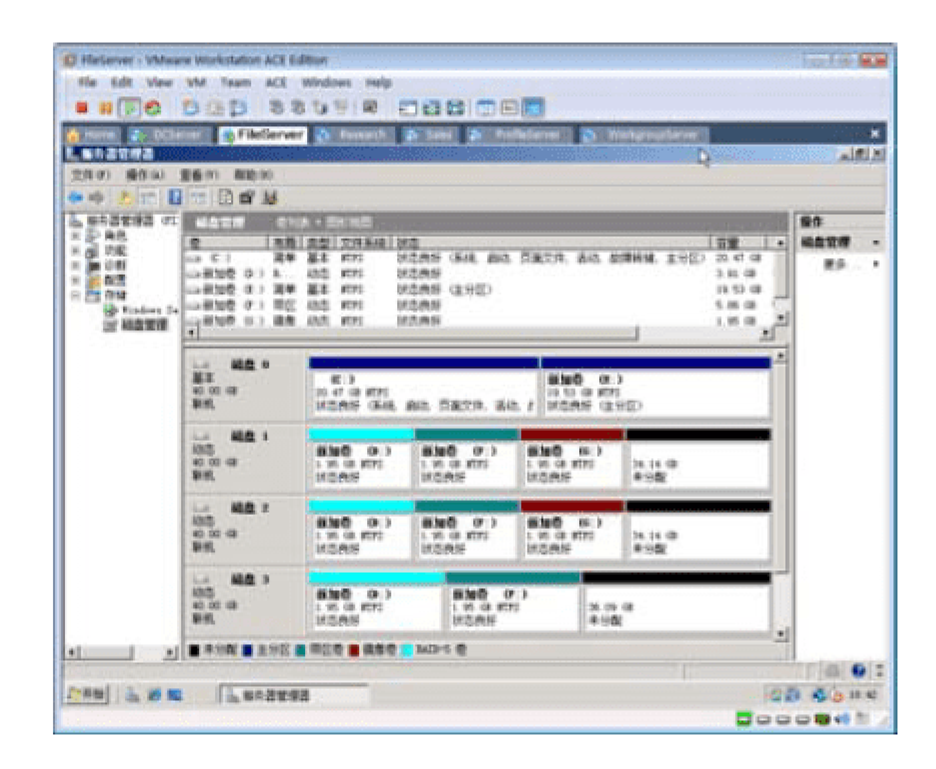


图 11-68　创建好的动态卷

11.6.1　模拟磁盘灾难

以下步骤将会删除磁盘 2，然后添加一个新的磁盘。

① 关闭 FileServer。

② 单击 Edit virtual machine settings。如图 11-69 所示，在出现的对话框中，选中 SecondDisk.vmdk，单击 Remove。删除一块硬盘，模拟硬盘坏掉。

③ 如图 11-69 所示，单击 Add 按钮。

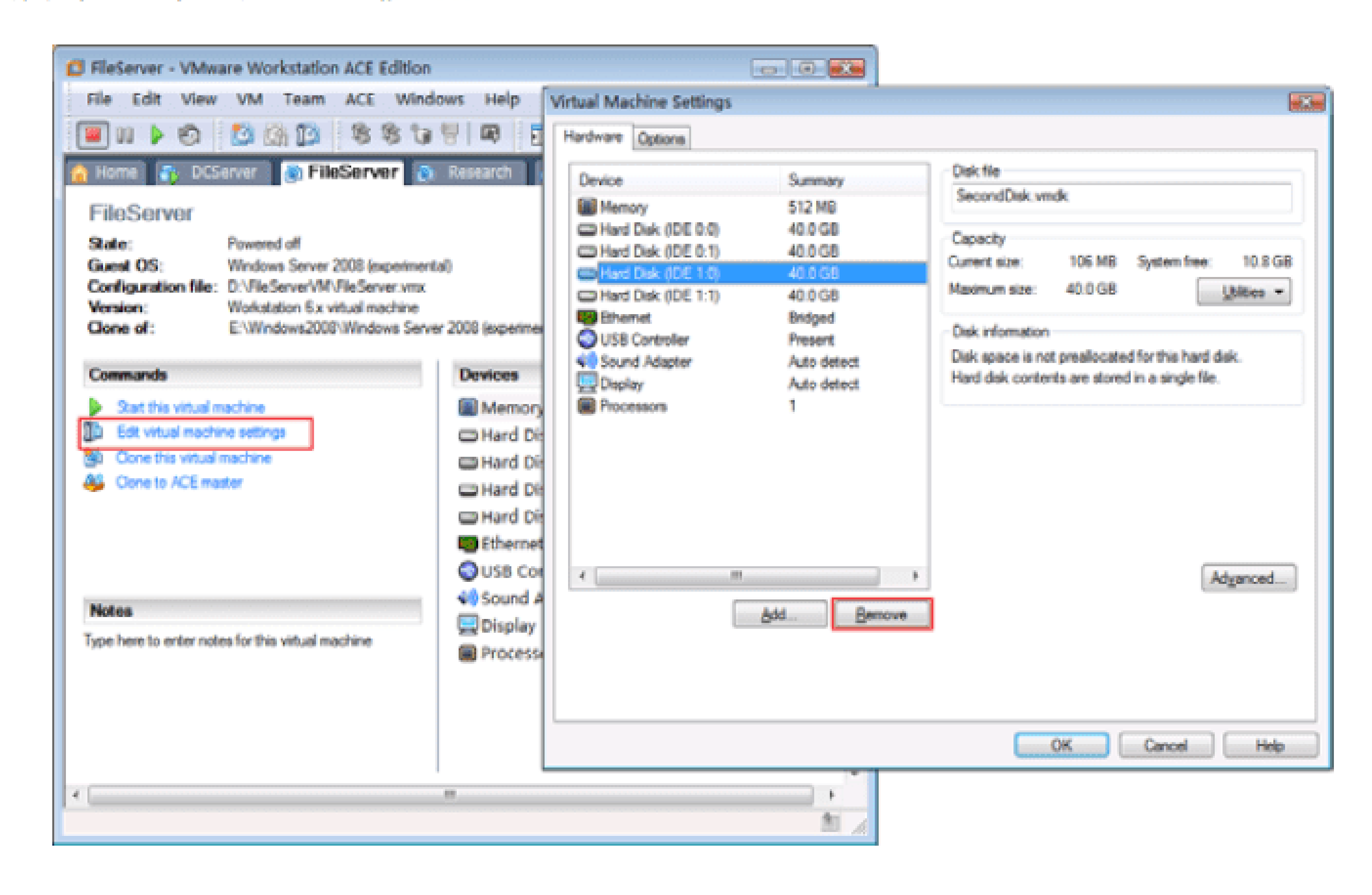
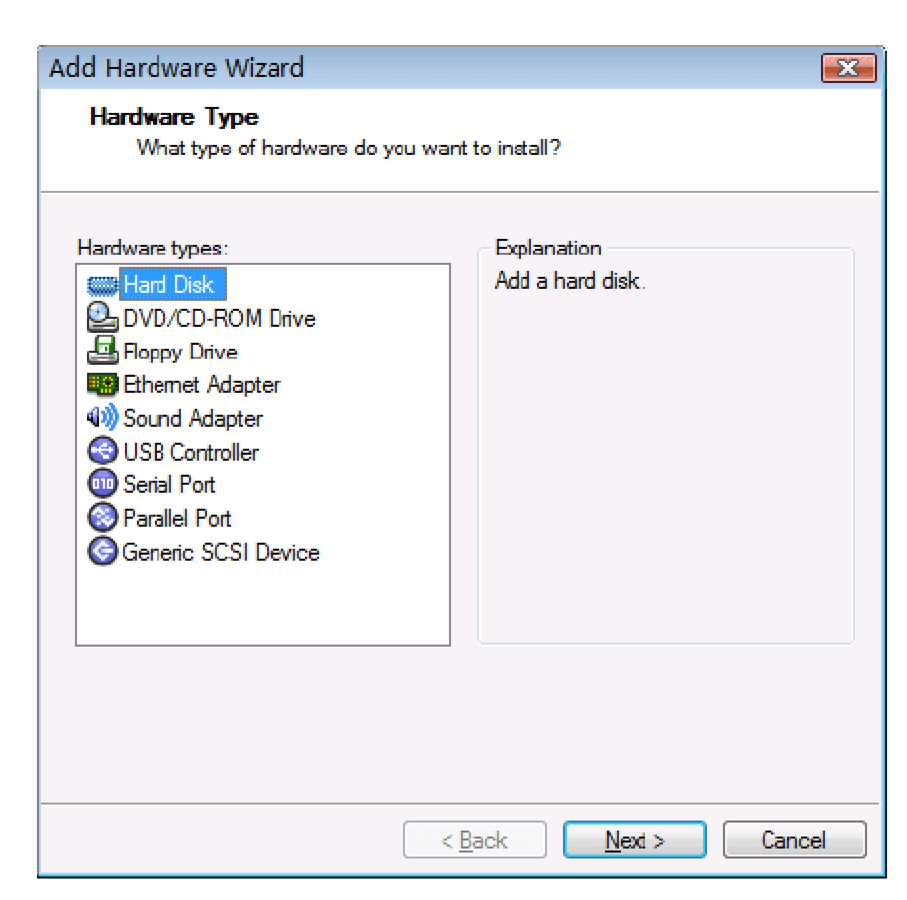


图 11-69　删除磁盘

④ 如图 11-70 所示，在出现的 Add Hardware Wizard(添加硬件向导)对话框中选中 Hard Disk，单击 Next 按钮。

⑤ 如图 11-71 所示，在 Select a Disk 界面中选中 Create a new virtual disk 单选按钮，单击 Next 按钮。



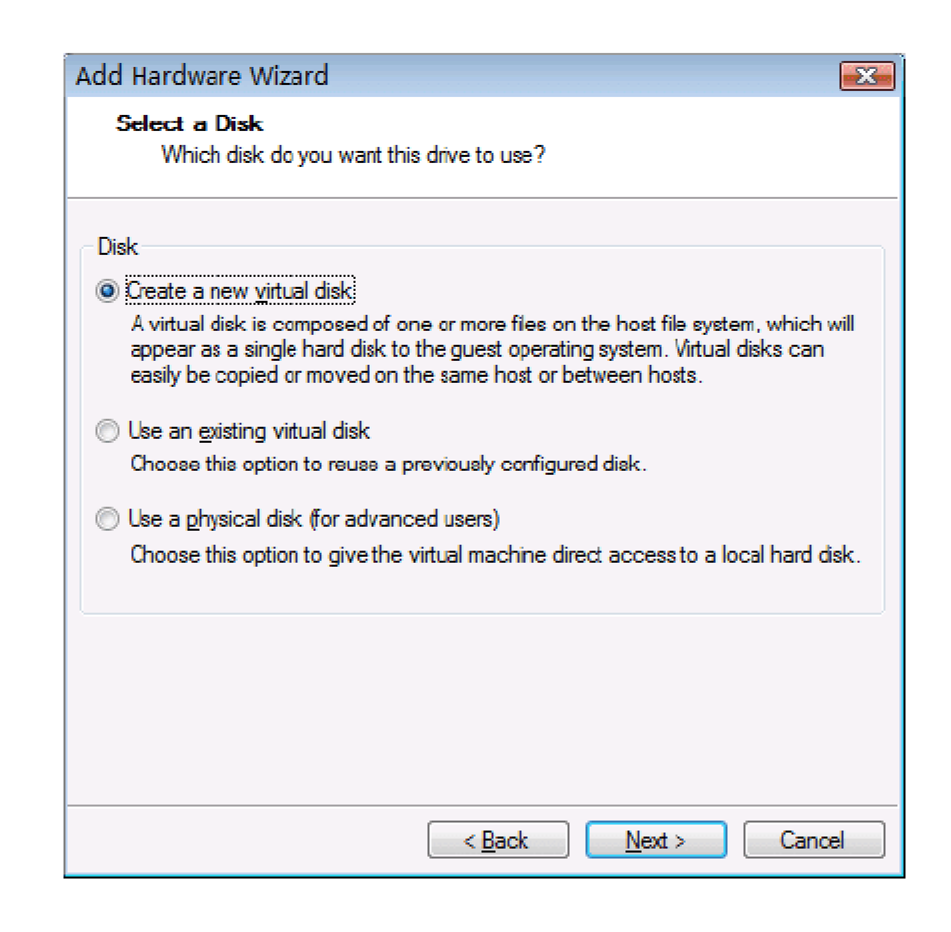



图 11-70　添加硬件

图 11-71　创建一个新的硬盘

⑥ 如图 11-72 所示，在出现的 Select a Disk Type 界面中选中 IDE 单选按钮，单击 Next 按钮。

⑦ 如图 11-73 所示，在出现的 Specify Disk File 界面中输入新的磁盘文件名称，单击 Next。模拟添

加了一块新的硬盘。

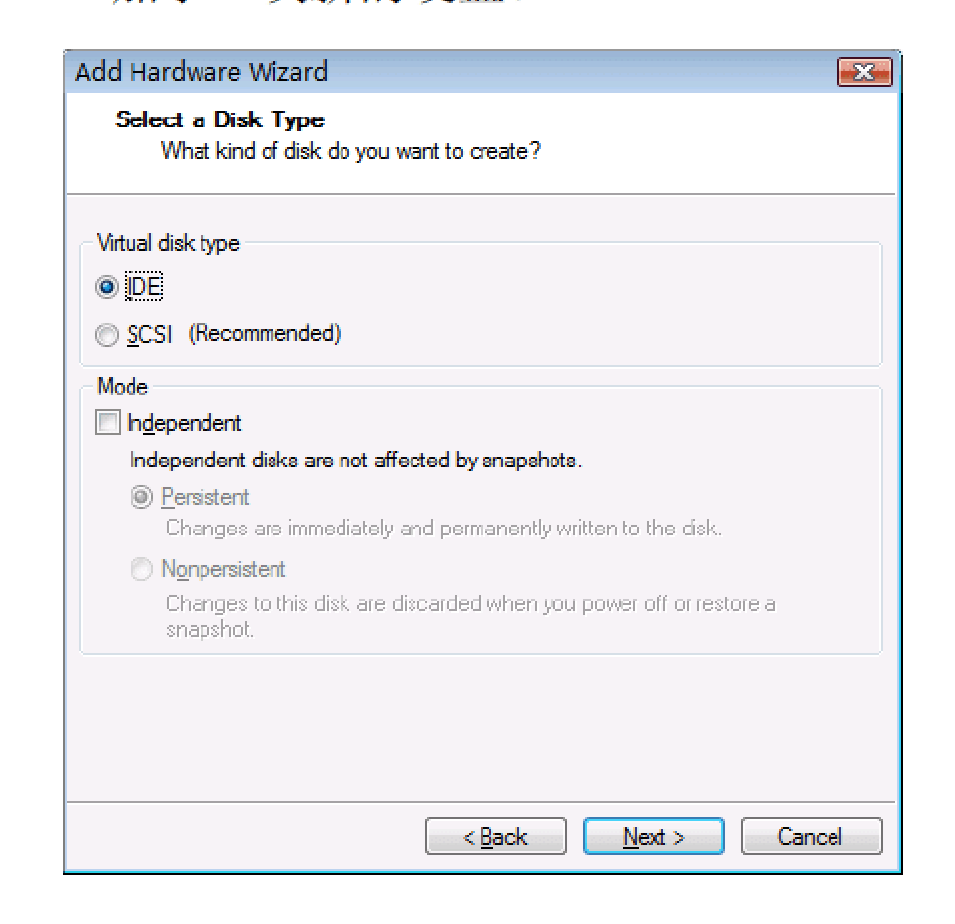


图 11-72　选择磁盘类型

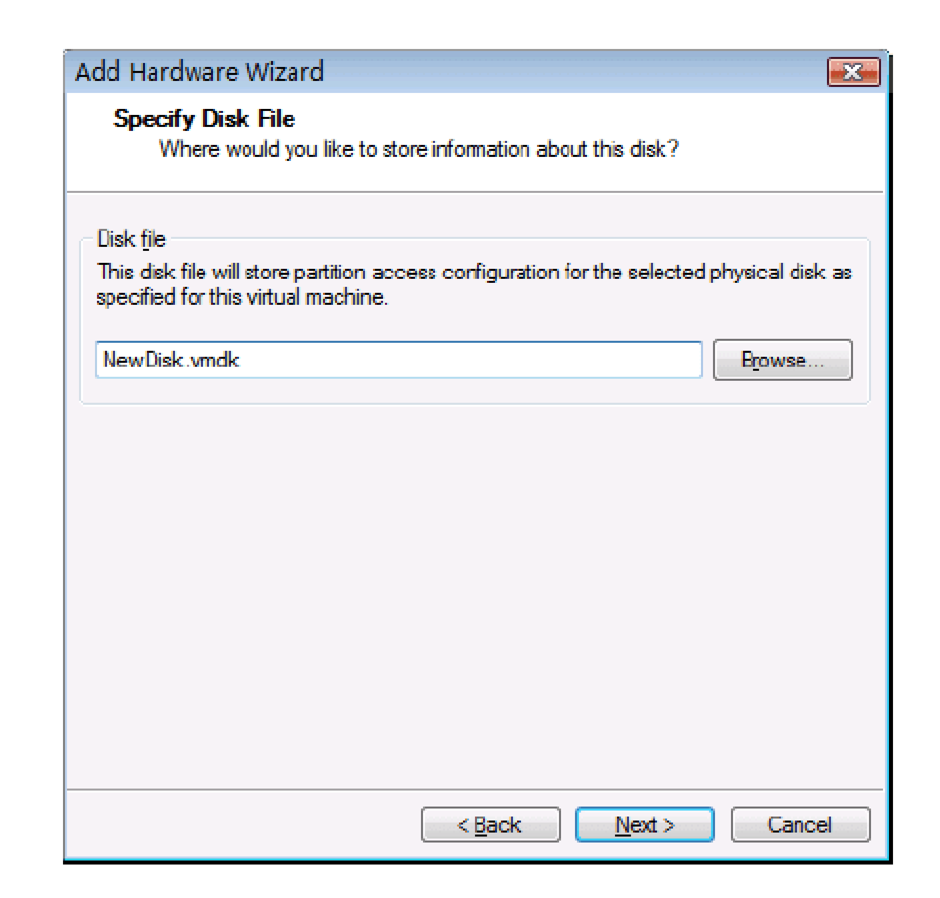


图 11-73　指定磁盘类型

⑧　如图 11-74 所示，在 Specify Disk Capacity 界面中输入磁盘大小 40，单击 Finish 按钮。

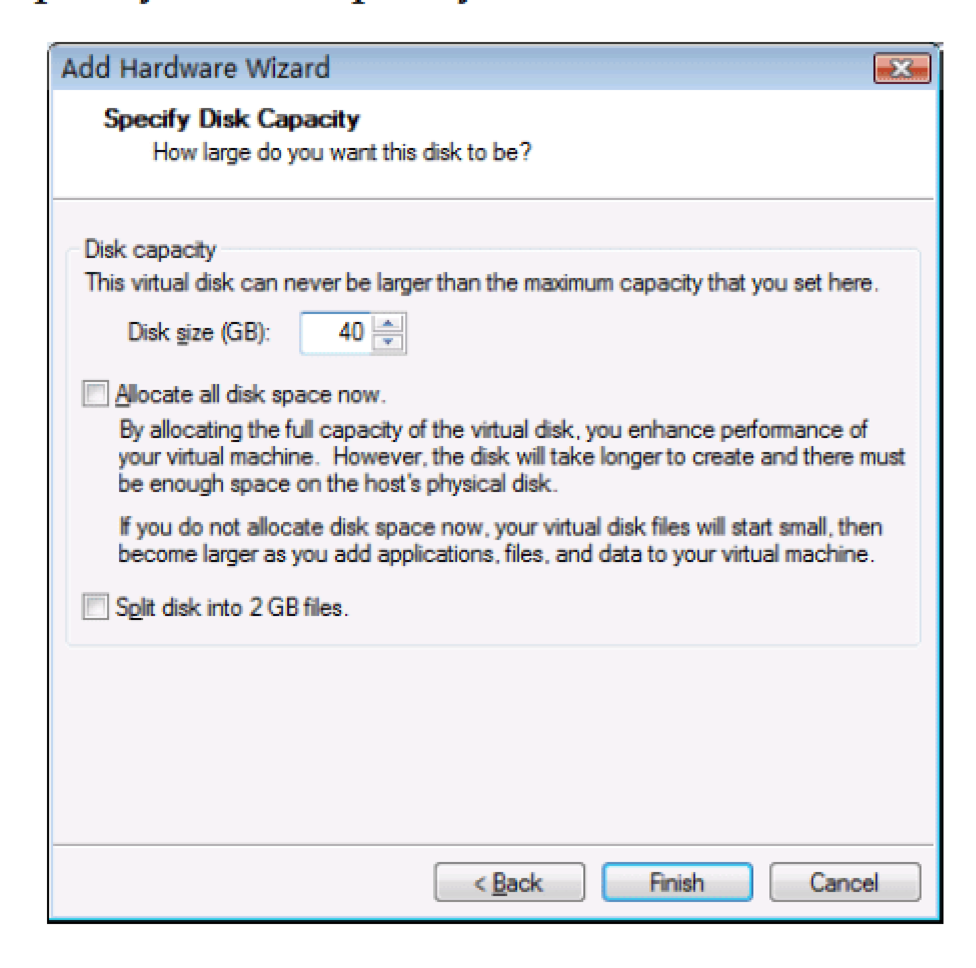


图 11-74　指定磁盘大小

11.6.2　修复镜像卷和 RAID-5

以下步骤将会演示将 RAID-5 和镜像卷恢复，确认带区卷的失败。

①　启动 FileServer。

②　以管理员身份登录，单击桌面上的“计算机”图标，如图 11-75 所示，可以看到 RAID-5 的卷 D、镜像卷 G 依然能够看见，并能够打开使用。

③　打开服务器管理器，展开“存储”→“磁盘管理”节点。

④　如图 11-76 所示，在出现的“初始化磁盘”对话框中，选中 MBR 单选按钮，单击“确定”按钮。

⑤　如图 11-77 所示，可以看到丢失的磁盘、新加的磁盘 2 以及失败的带区卷。可以看到 RAID-5 卷 D，状态是“失败的重复”，带区卷的状态是“失败”，镜像卷 G 的状态是“失败的重复”。

⑥　如图 11-78 所示，右击 D 卷，从弹出的快捷菜单中选择“修复卷”命令。

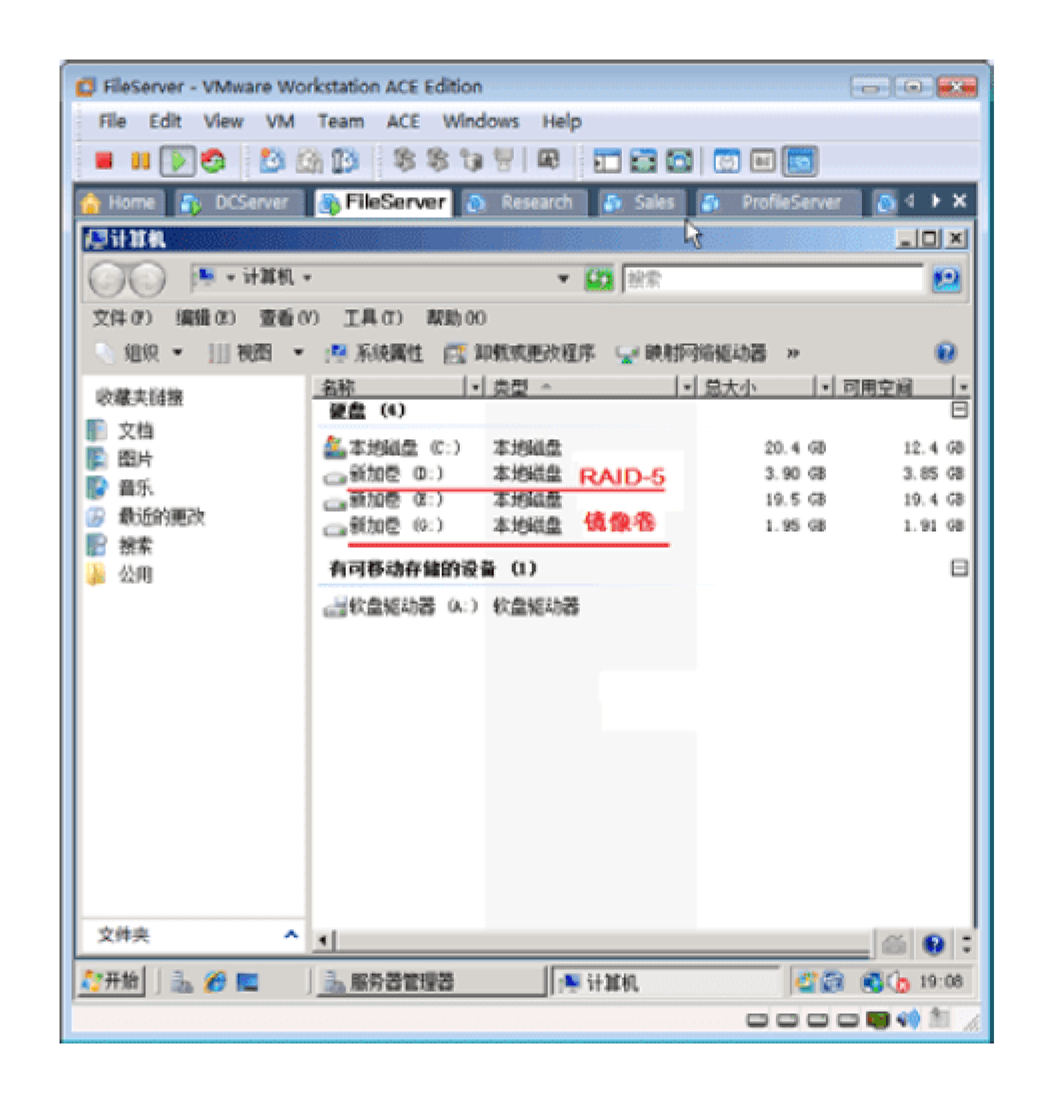


图 11-75　能够访问的卷

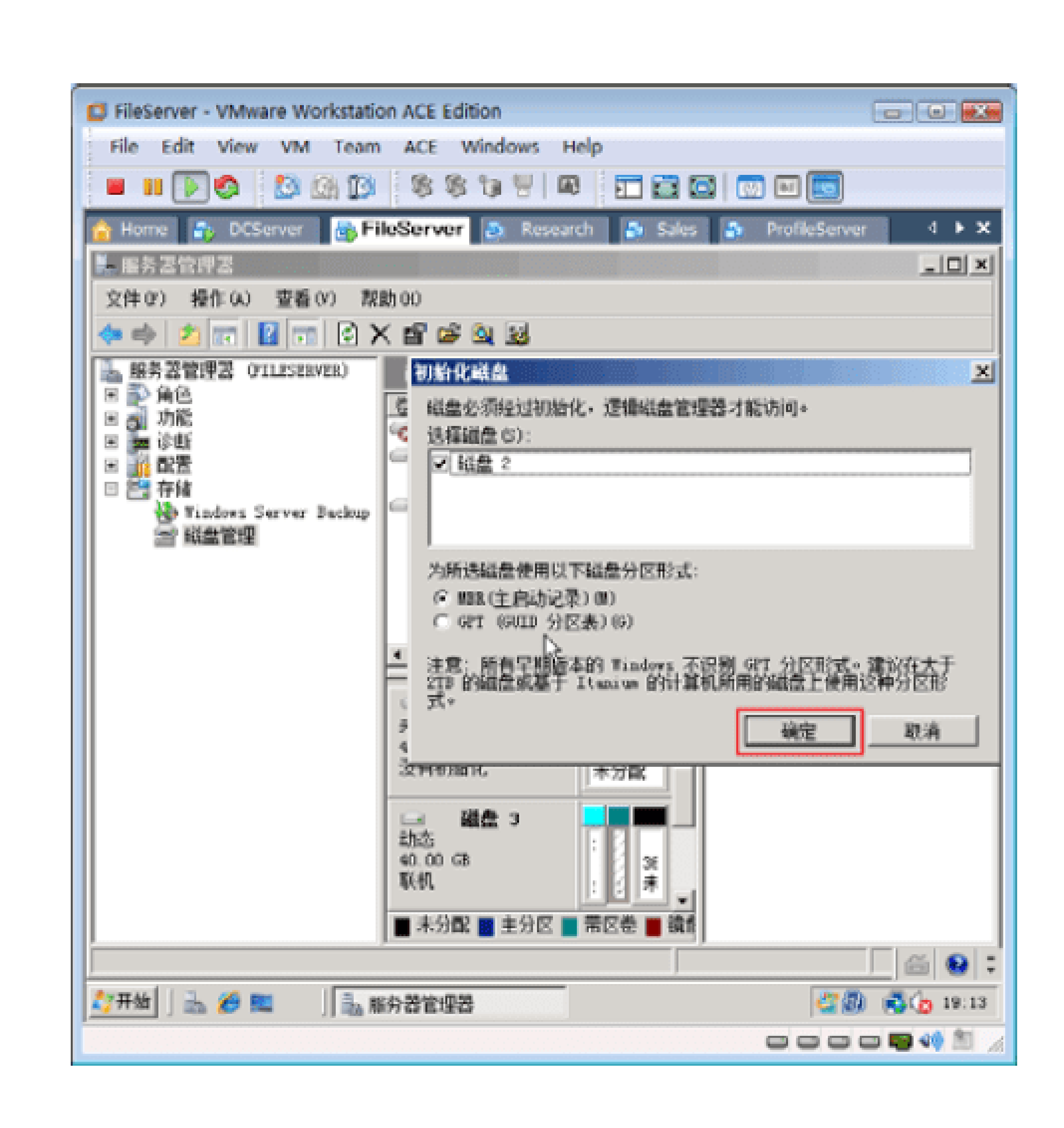


图 11-76　初始化磁盘

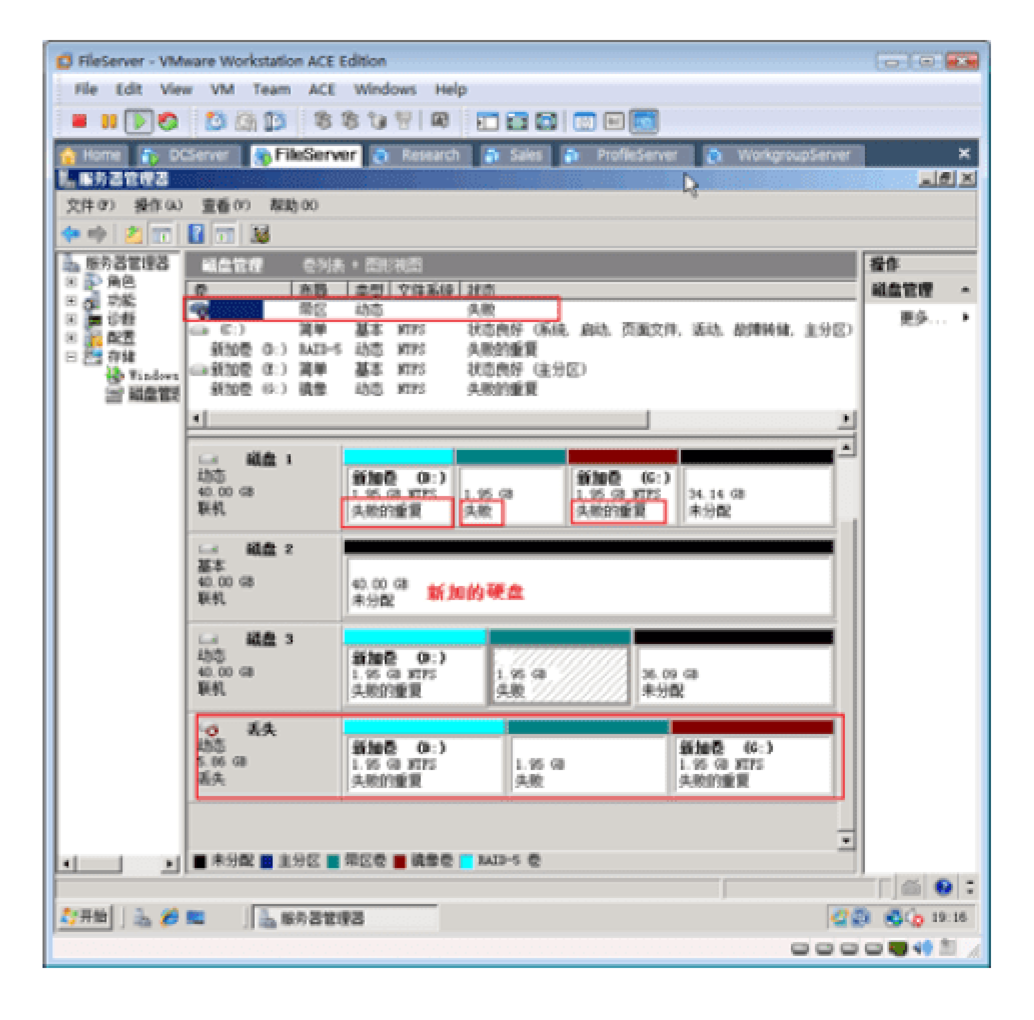


图 11-77 失败的卷

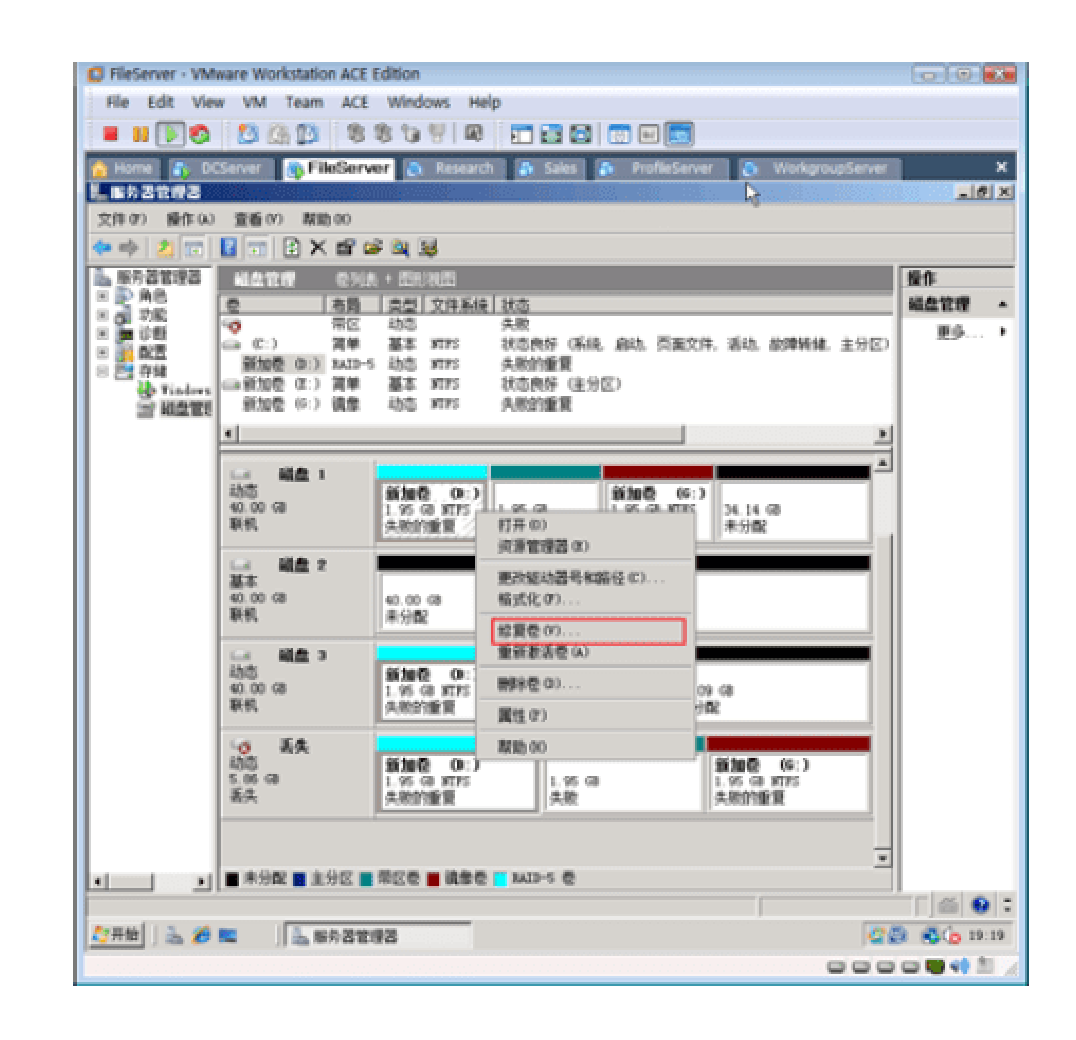


图 11-78　修复卷 RAID-5

⑦　如图 11-79 所示，在出现的对话框中选中磁盘 2，单击“确定”按钮。

⑧　如图 11-80 所示，在出现的提示框中单击“是”按钮，将磁盘 2 转换成动态磁盘。

⑨　如图 11-81 所示，可以看到 RAID-5 D 卷的状态已经变成“状态良好”。

⑩　如图 11-82 所示，右击镜像卷，从弹出的快捷菜单中选择“删除镜像”命令。

⑪　如图 11-83 所示，在“删除镜像”对话框中选中丢失的磁盘，单击“删除镜像”按钮，在出现的提示框中单击“是”按钮。

⑫　如图 11-84 所示，右击简单卷 G，从弹出的快捷菜单中选择“添加镜像”命令。

⑬　如图 11-85 所示，在出现的“添加镜像”对话框中选中磁盘 2，单击“添加镜像”按钮。

⑭　如图 11-86 所示，可以看到，镜像卷 G 的状态为“状态良好”。

⑮　如图 11-87 所示，右击失败的带区卷，在弹出的快捷菜单中选择“删除卷”命令。在出现的提示框中，单击“是”按钮。

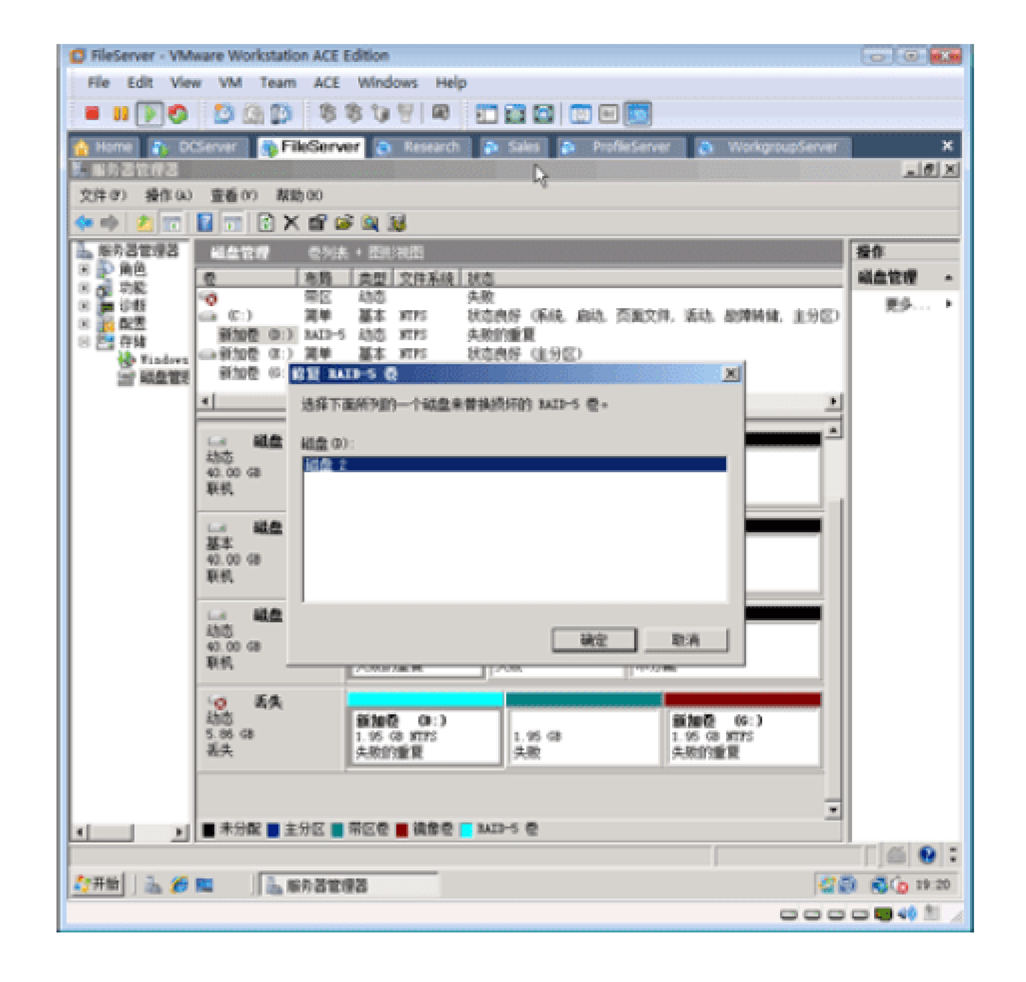


图 11-79　选择磁盘

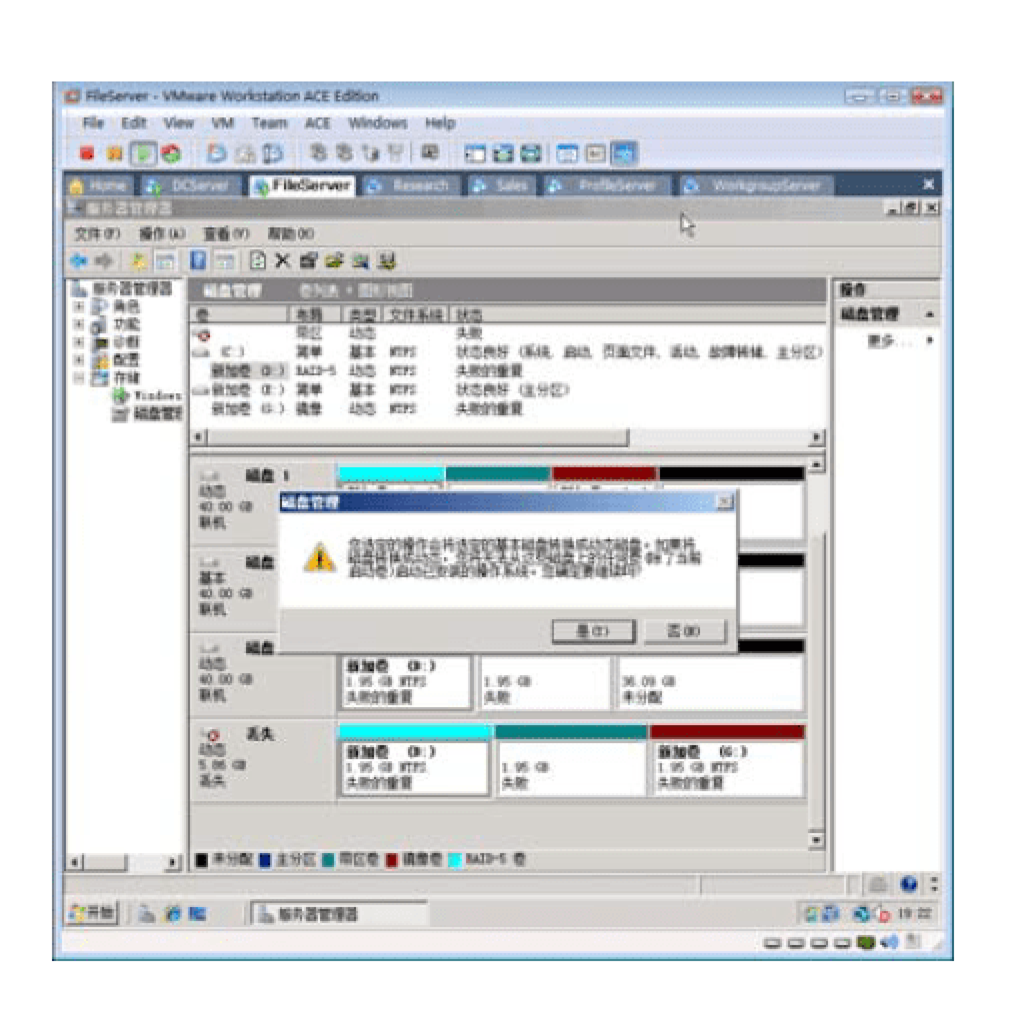


图 11-80　转换成动态磁盘

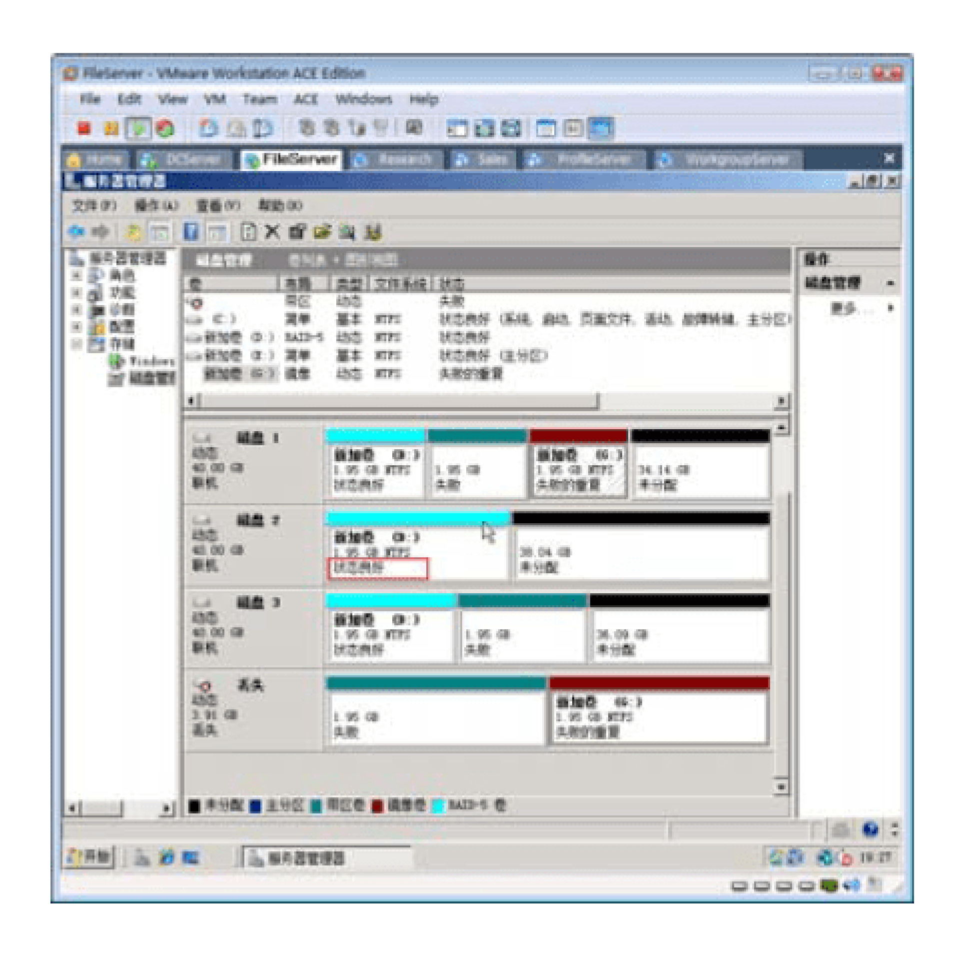


图 11-81　修复好的 RAID-5

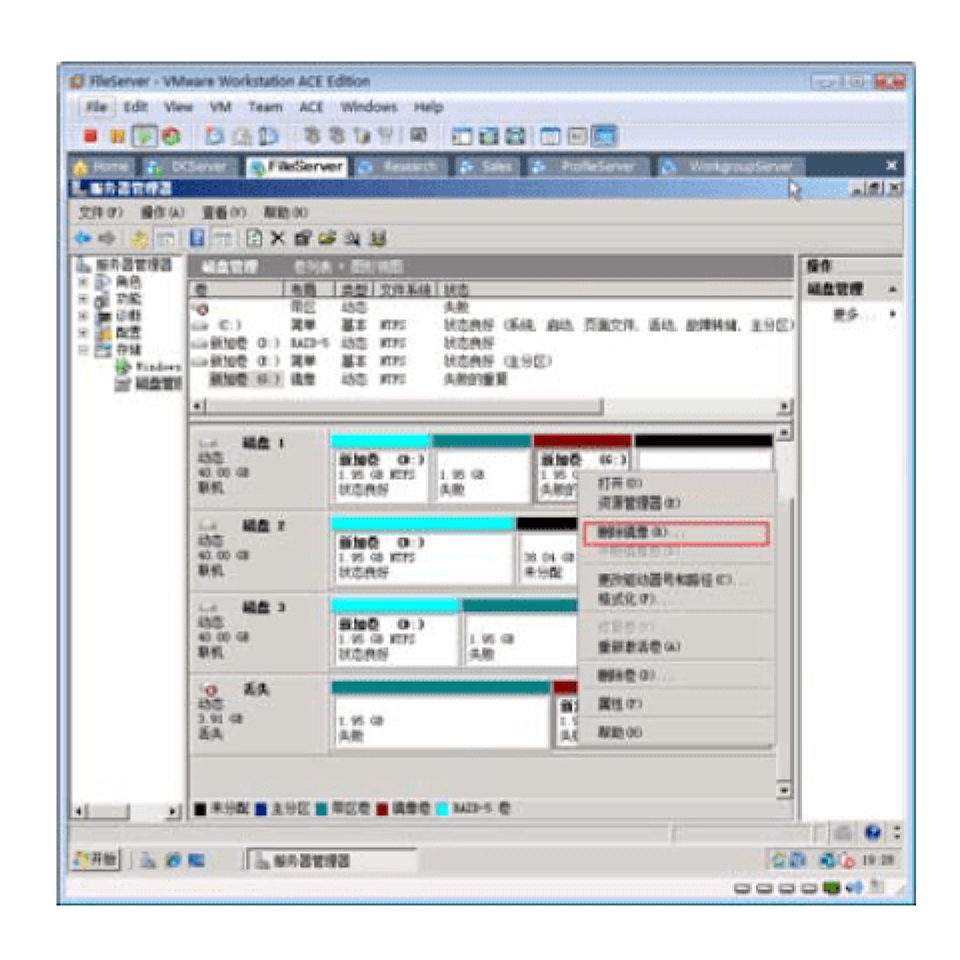


图 11-82　删除镜像

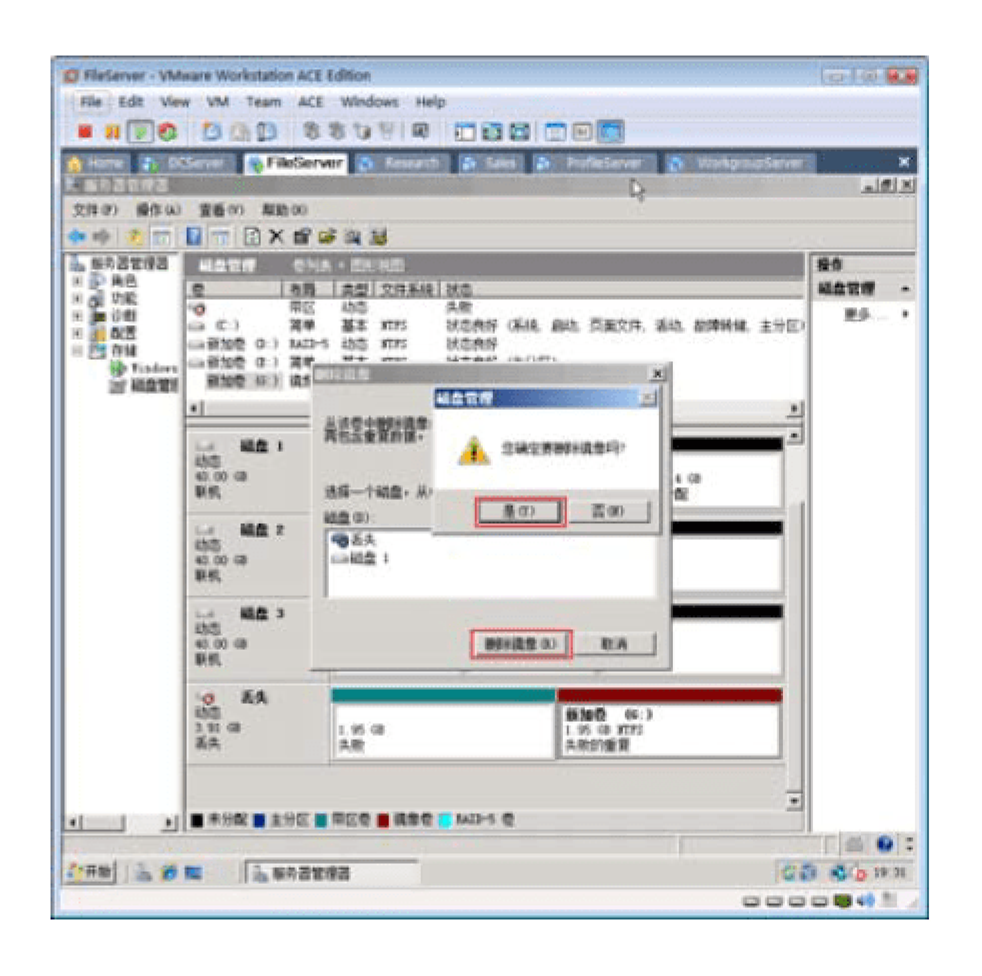


图 11-83　选中丢失的盘

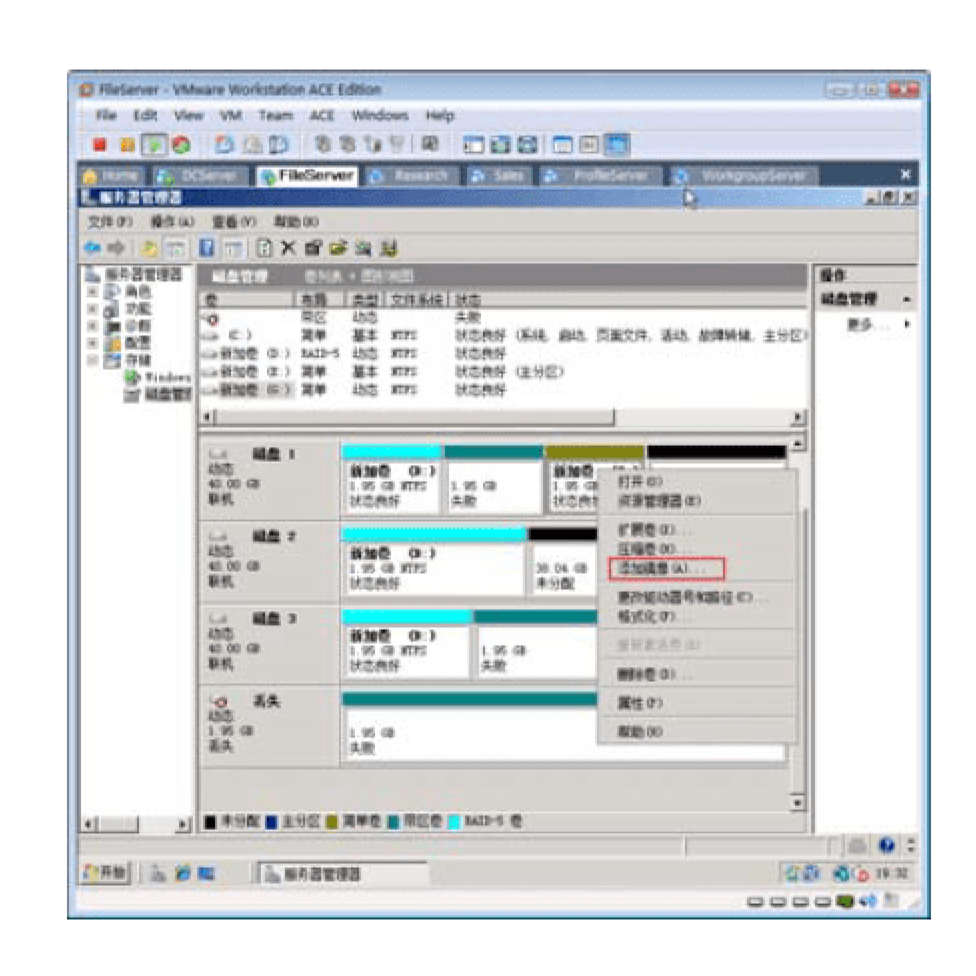


图 11-84　添加镜像

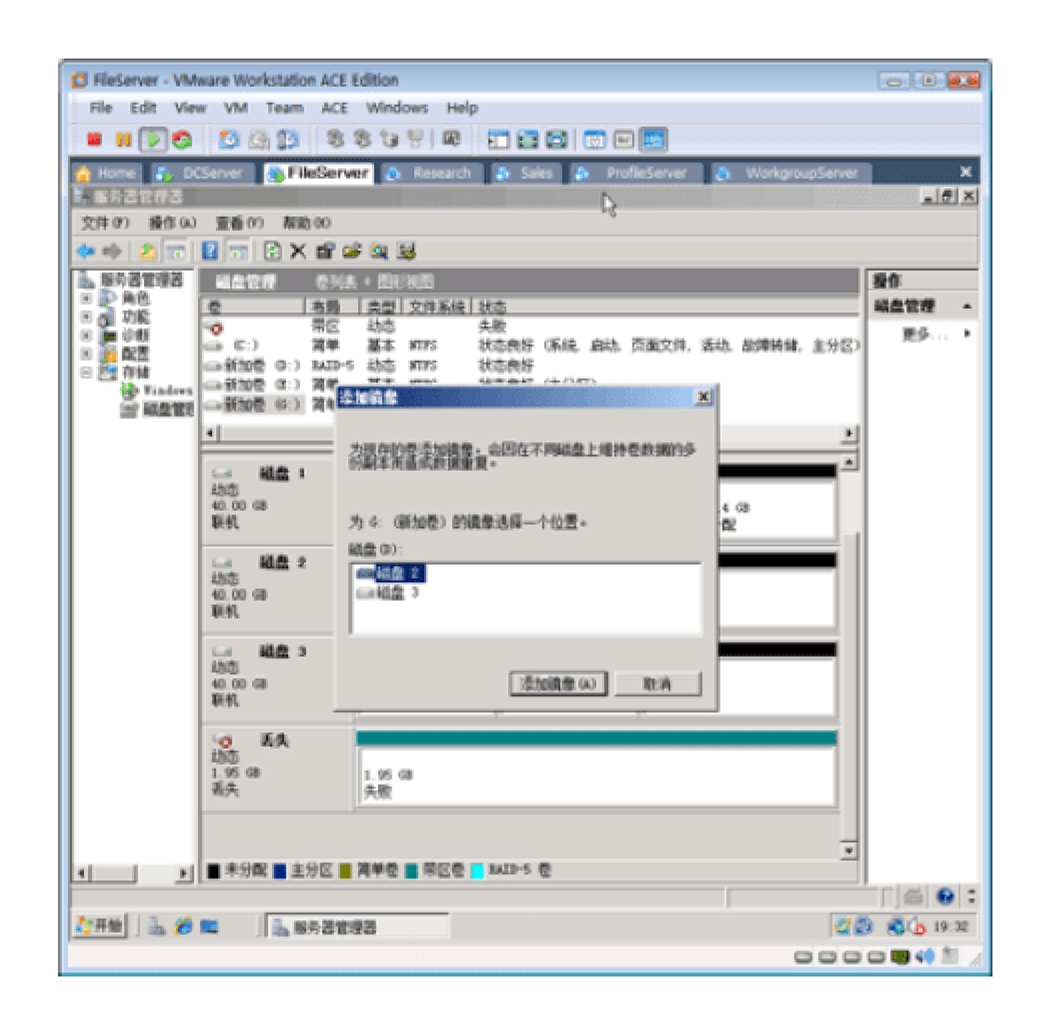


图 11-85　选择磁盘

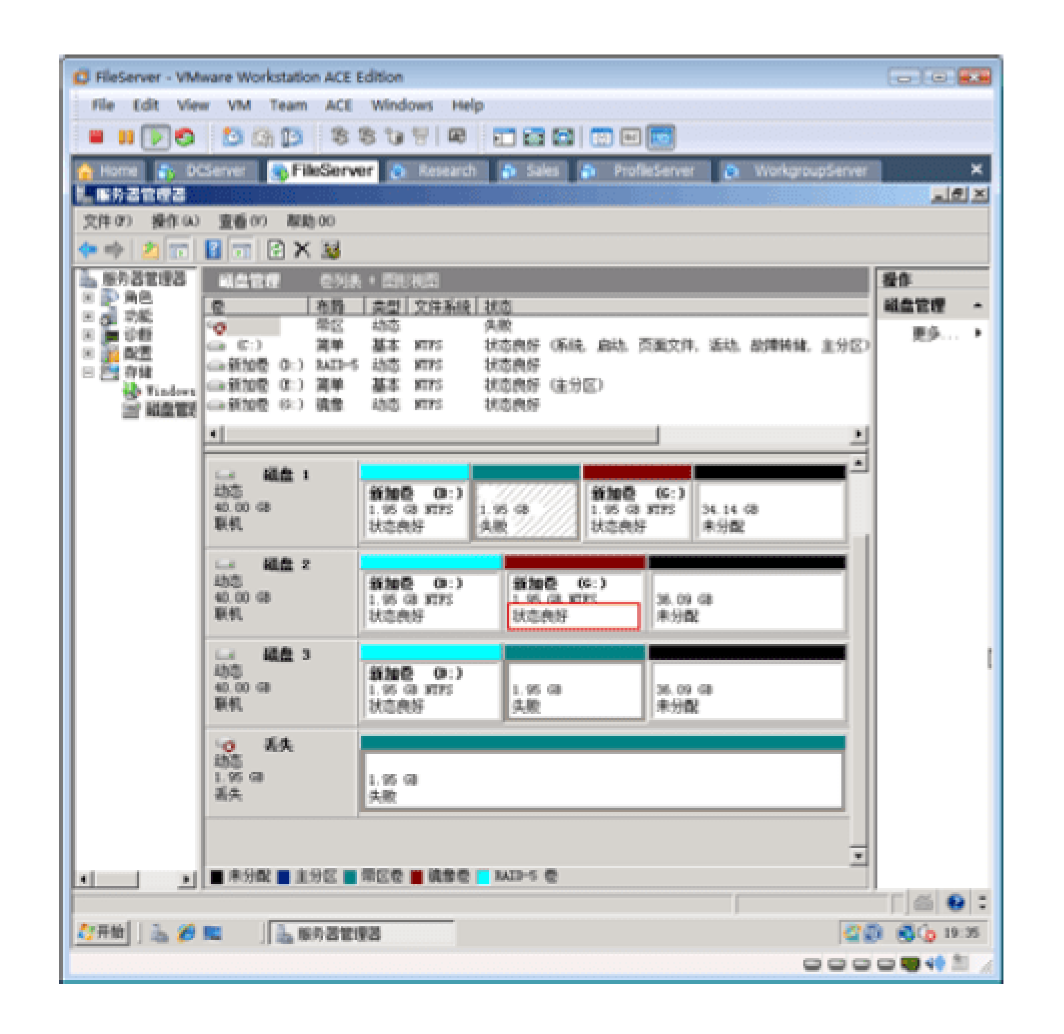


图 11-86　修复好的 RAID-1

⑯　关闭服务器管理器，再次打开。

⑰　如图 11-88 所示，右击丢失的磁盘，从弹出的快捷菜单中选择“删除磁盘”命令。

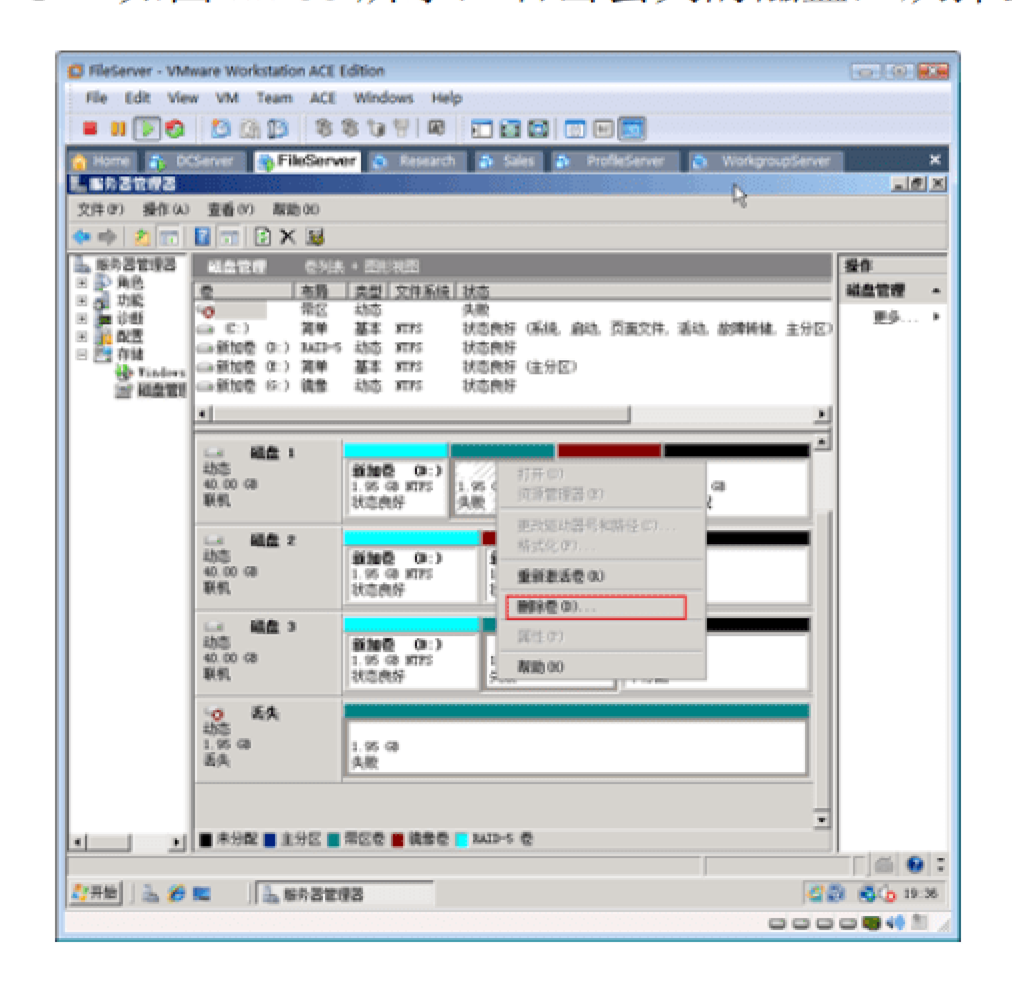


图 11-87　删除失败的带区卷

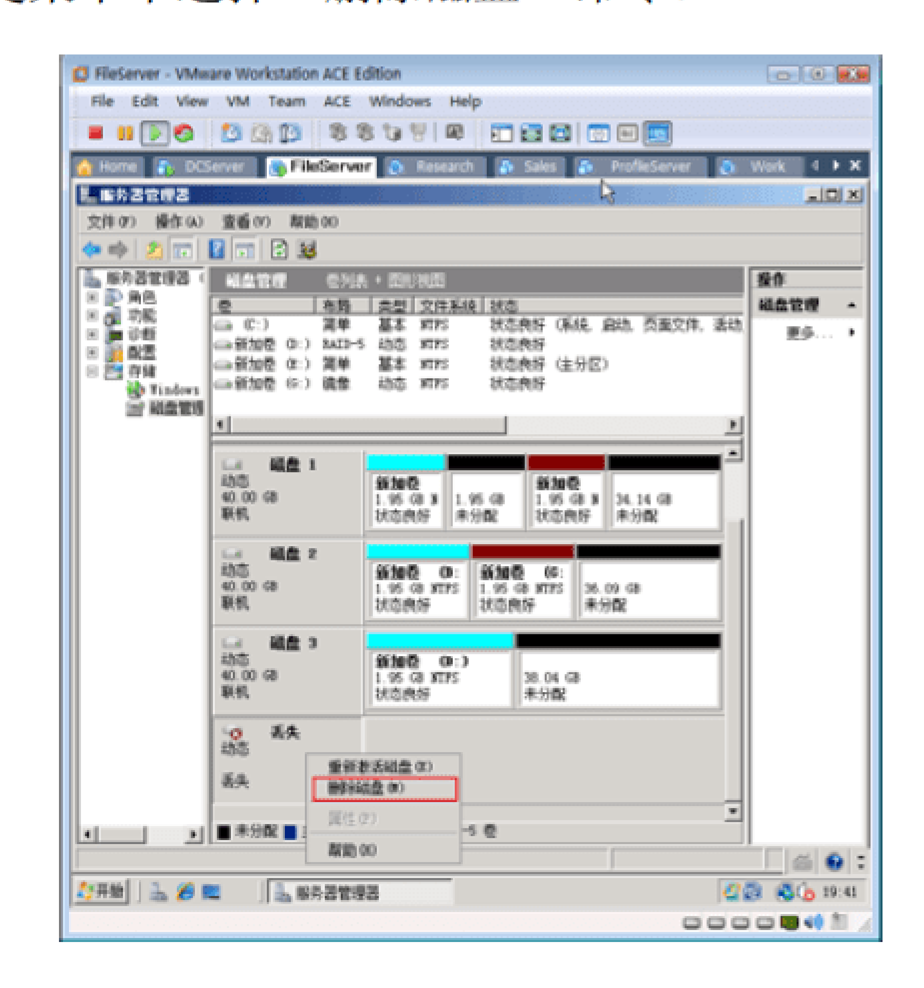


图 11-88　删除丢失的磁盘

11.7　远程管理 Windows Server Core 的磁盘

在 Windows Server Core 的操作系统上没有图形界面的管理工具来管理磁盘，而使用命令行创建和管理动态磁盘有些复杂，现在介绍使用其他服务器上的磁盘管理工具管理 Windows Server Core 的磁盘。

ProfileServer 是安装了 Windows Server Core 的文件服务器。下面将会演示如何使用 Research 计算机上的磁盘管理工具管理 ProfileServer 的磁盘。

①　关闭 ProfileServer。

②　添加两块 40 MB 的 IDE 接口的硬盘。

③ 启动 ProfileServer、DCserver 和 Research。

④ 以域管理员身份登录到 Research 计算机。

⑤ 选择“开始”→“运行”命令，在出现的“运行”对话框中输入 mmc，单击“确定”按钮。

⑥ 如图 11-89 所示，在打开的控制台窗口，选择“文件”→“添加\删除管理单元”命令。

⑦ 如图 11-90 所示，在出现的“添加/删除管理单元”对话框中，选中“磁盘管理”，单击“添加”按钮。

⑧ 如图 11-90 所示，在“选择计算机”界面中，选中“以下计算机”单选按钮，输入 profileserver，单击“完成”按钮。

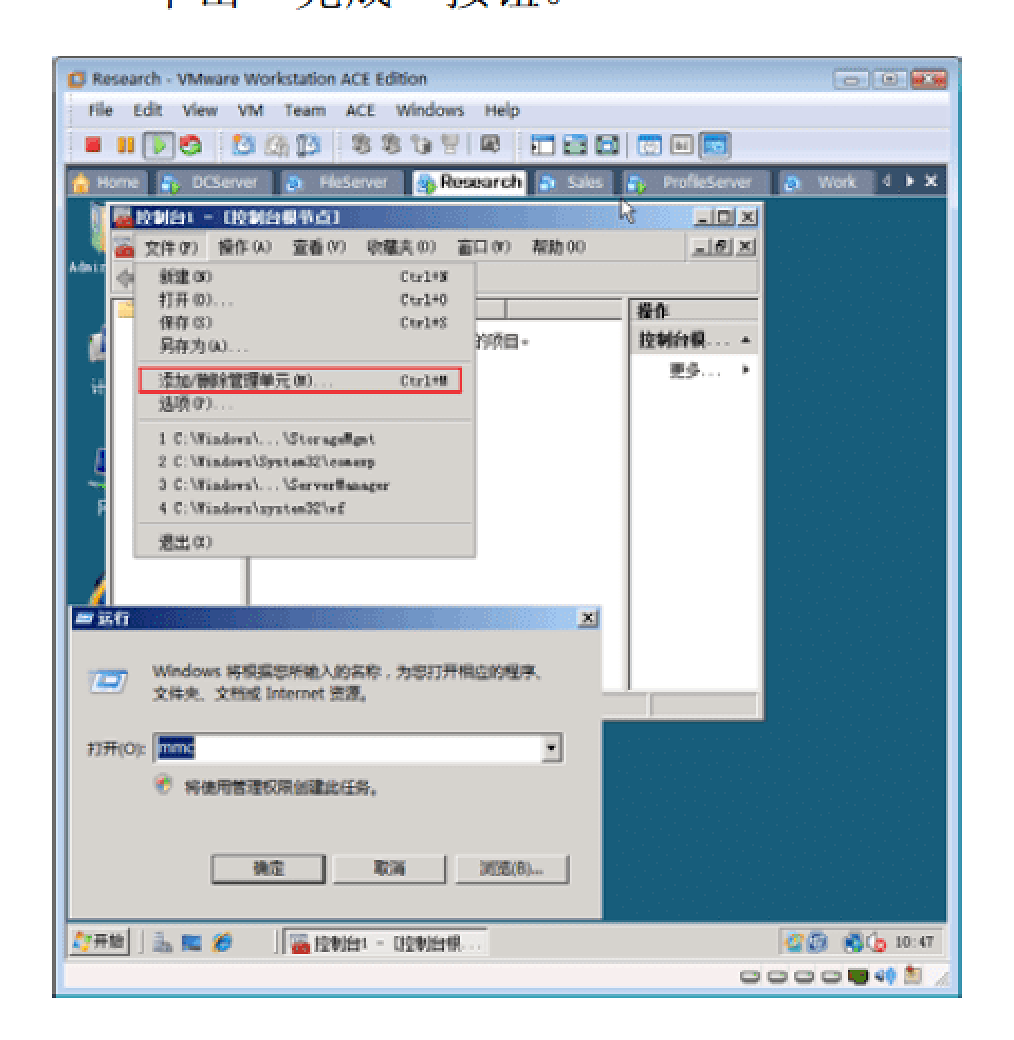


图 11-89 添加删除管理单元

图 11-90 选择磁盘管理

⑨ 如图 11-91 所示，单击“磁盘管理”按钮，在出现的“初始化磁盘”对话框中选中磁盘 0 和磁盘 1，选中 MBR 单选按钮，单击“确定”按钮。

⑩ 明明已经初始化过了，但是我们发现磁盘 0 和磁盘 1 提示还是没有初始化。这是因为状态没有刷新过来，必须保存管理工具，再次打开才能刷新，如图 11-92 所示。

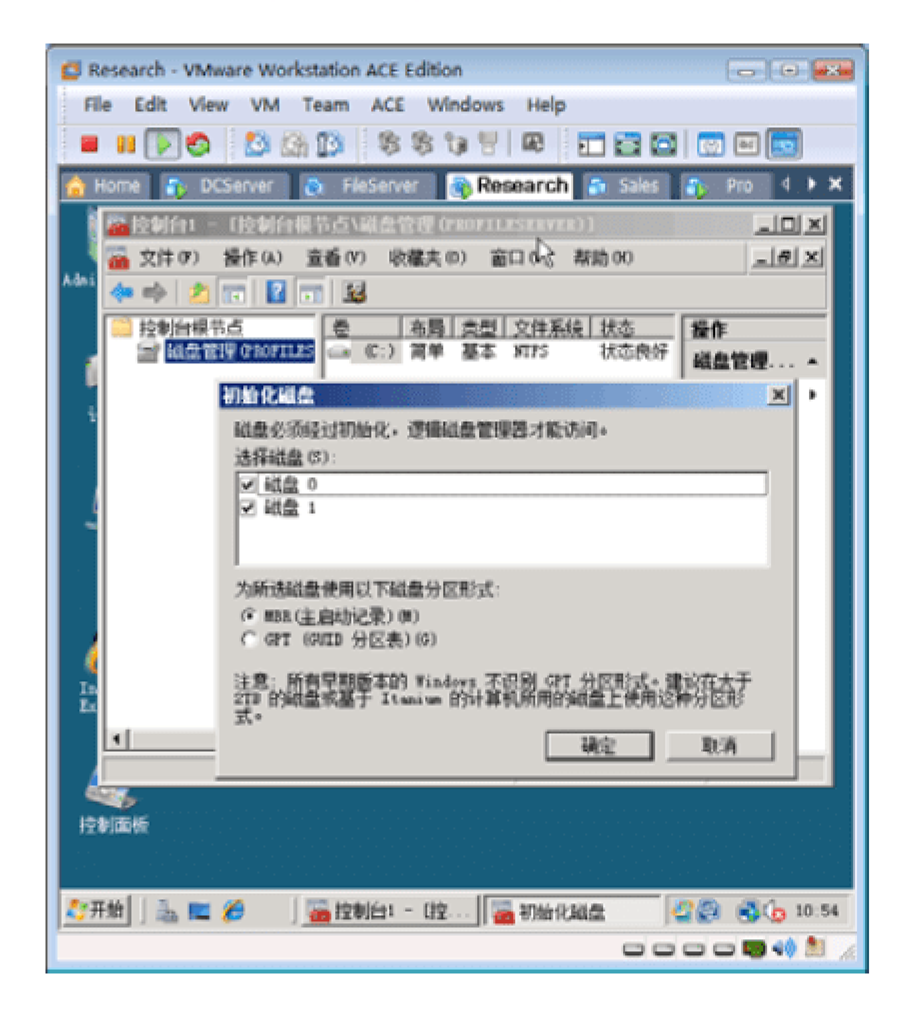


图 11-91 初始化磁盘

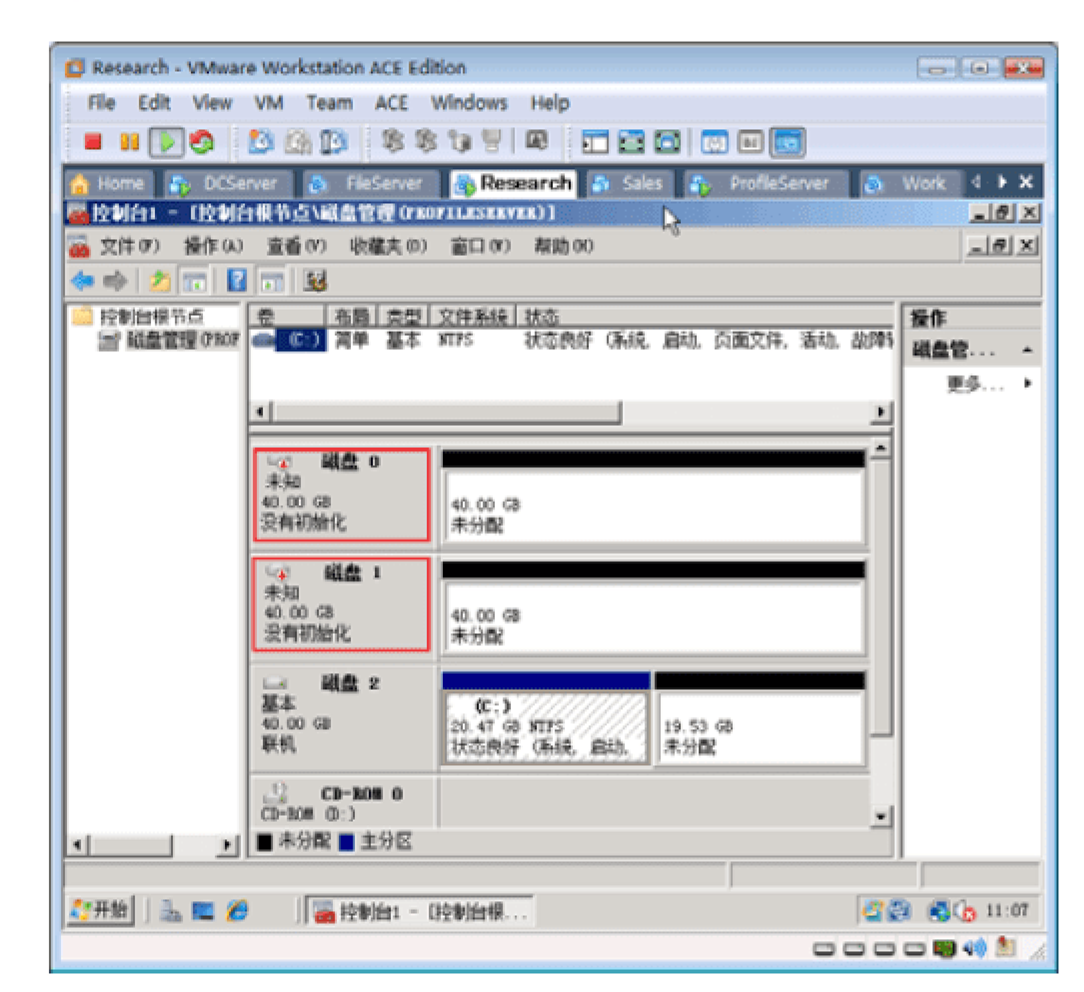


图 11-92 刷新状态

⑪ 如图 11-93 所示，选择“文件”→“保存”命令，输入 profileServerDiskManager，单击“保存”按钮。

⑫ 如图 11-94 所示，关闭这个管理工具，选择“开始”→“程序”→“管理工具”→ profileServerDiskManager 命令，可以看到磁盘的状态已经是“联机”。

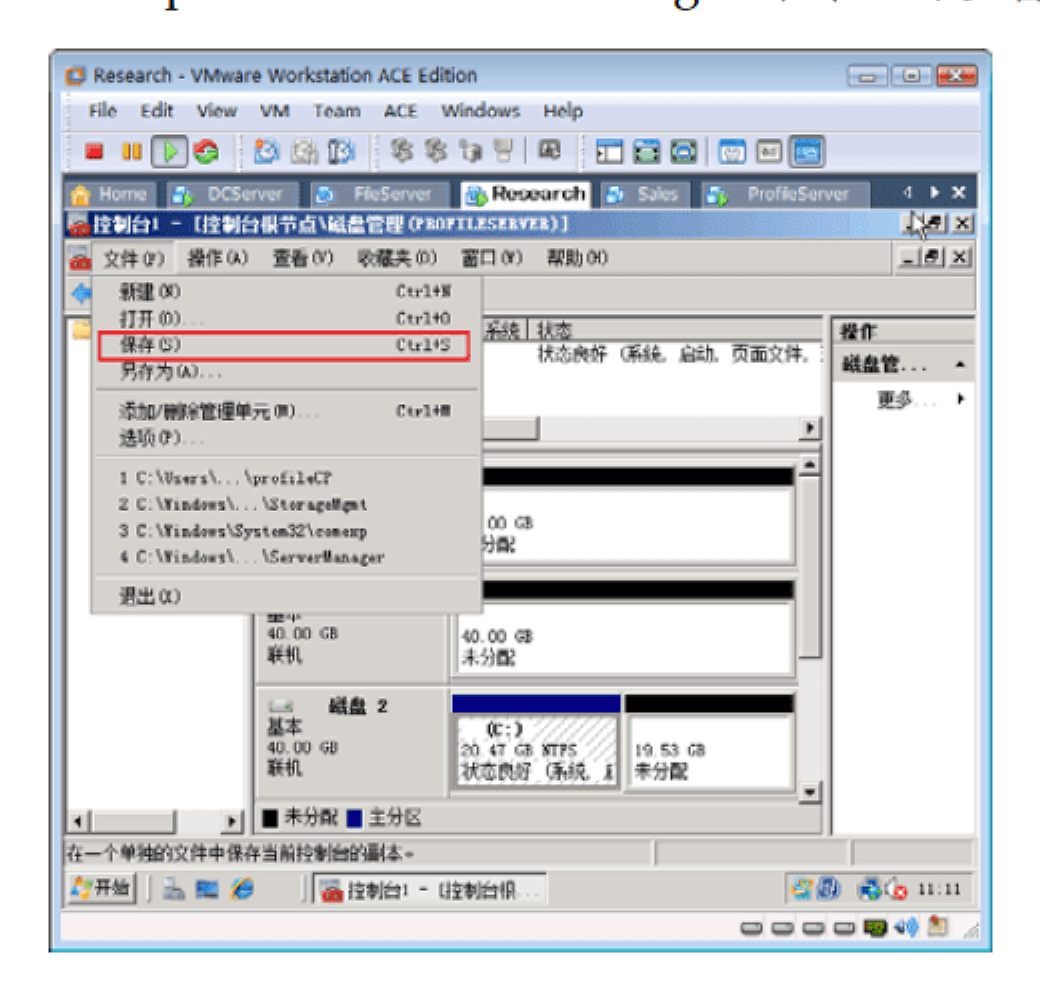


图 11-93　保存管理工具

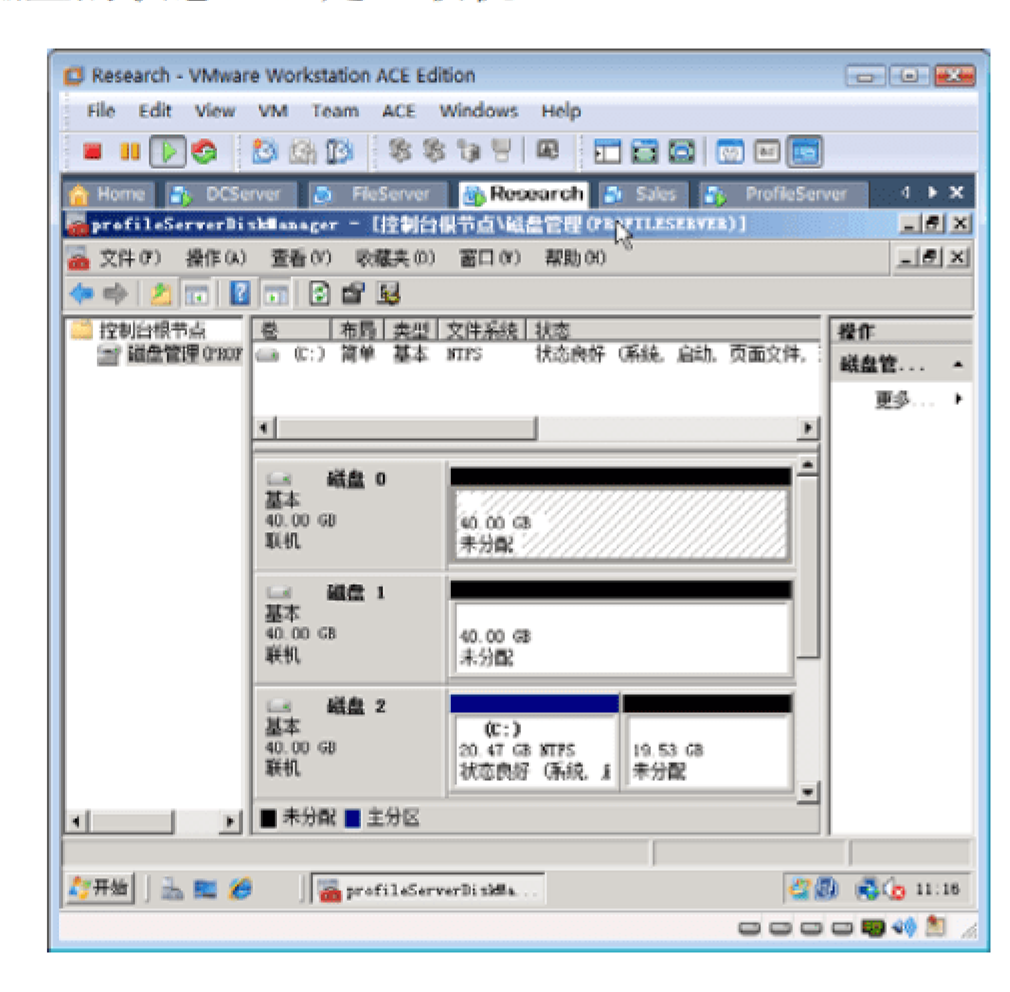


图 11-94　磁盘状态

⑬ 以后就可以像管理本地磁盘一样管理 Windows Server Core 上的磁盘了。如果你发现你的操作没有生效，需要关闭管理工具，然后再次打开，就能看到变化了。

⑭ 如图 11-95 所示，已将磁盘 0 和磁盘 1 创建了一个镜像卷 E。

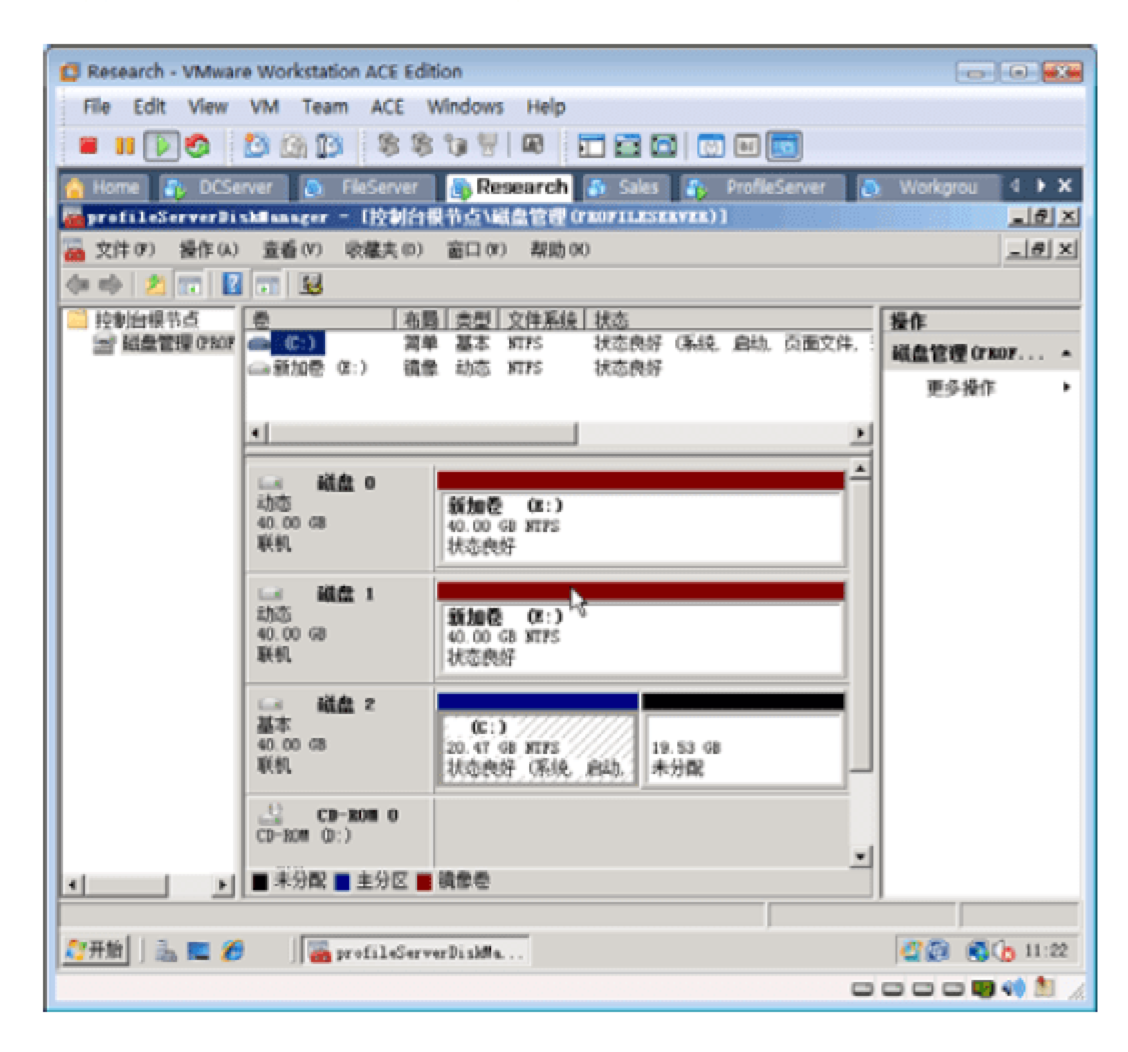


图 11-95　创建分区格式化分区

⑮ 将基本磁盘转换成动态磁盘，重新打开管理工具。

⑯ 创建镜像卷，重新打开管理工具。

⑰ 指定盘符，重新打开管理工具。现在你终于可以看到创建好的镜像卷了。

11.8 动态磁盘迁移

如果 FileServer 主板坏掉了，需要将 3 块动态磁盘接到 Research 服务器上。

该运行 Research 的计算机必须将这几个动态磁盘上的镜像卷和 RAID-5 卷同步，用户才能使用。

① 关闭 FileServer。

② 单击 Edit virtual machine settings，如图 11-96 所示，在出现的 Virtual Machine Settings 对话框中选中 FirstDisk.vmdk，单击 Remove 按钮。

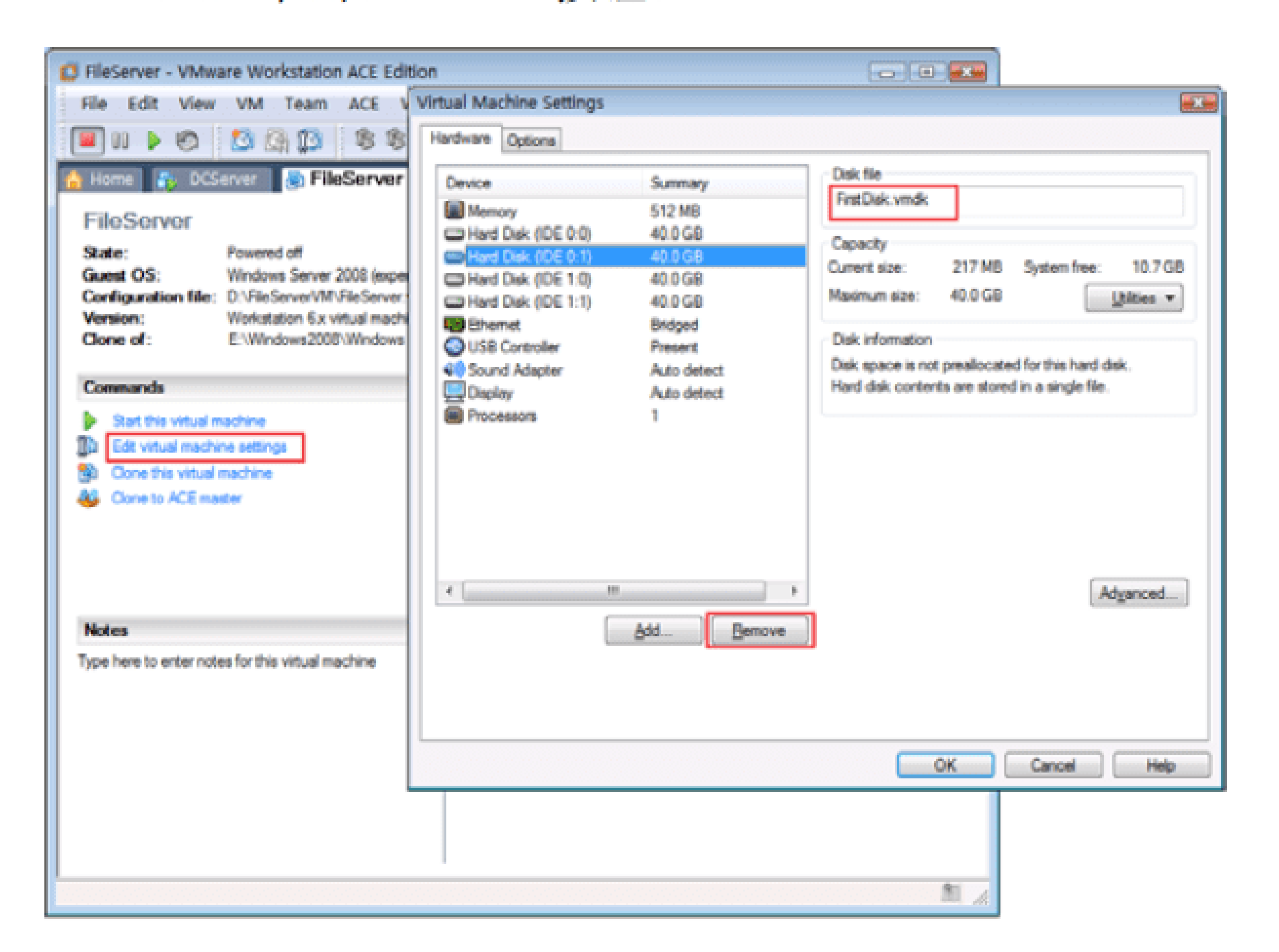


图 11-96 删除磁盘

③ 选中 NewDisk.vmdk，单击 Remove 按钮。

④ 选中 thirdDisk.vmdk，单击 Remove 按钮。

⑤ 如图 11-97 所示，切换到 Research 选项卡，单击 Edit virtual machine settings，在出现的 Virtual Machine Settings 对话框中选中 CD-ROM，单击 Remove 按钮。

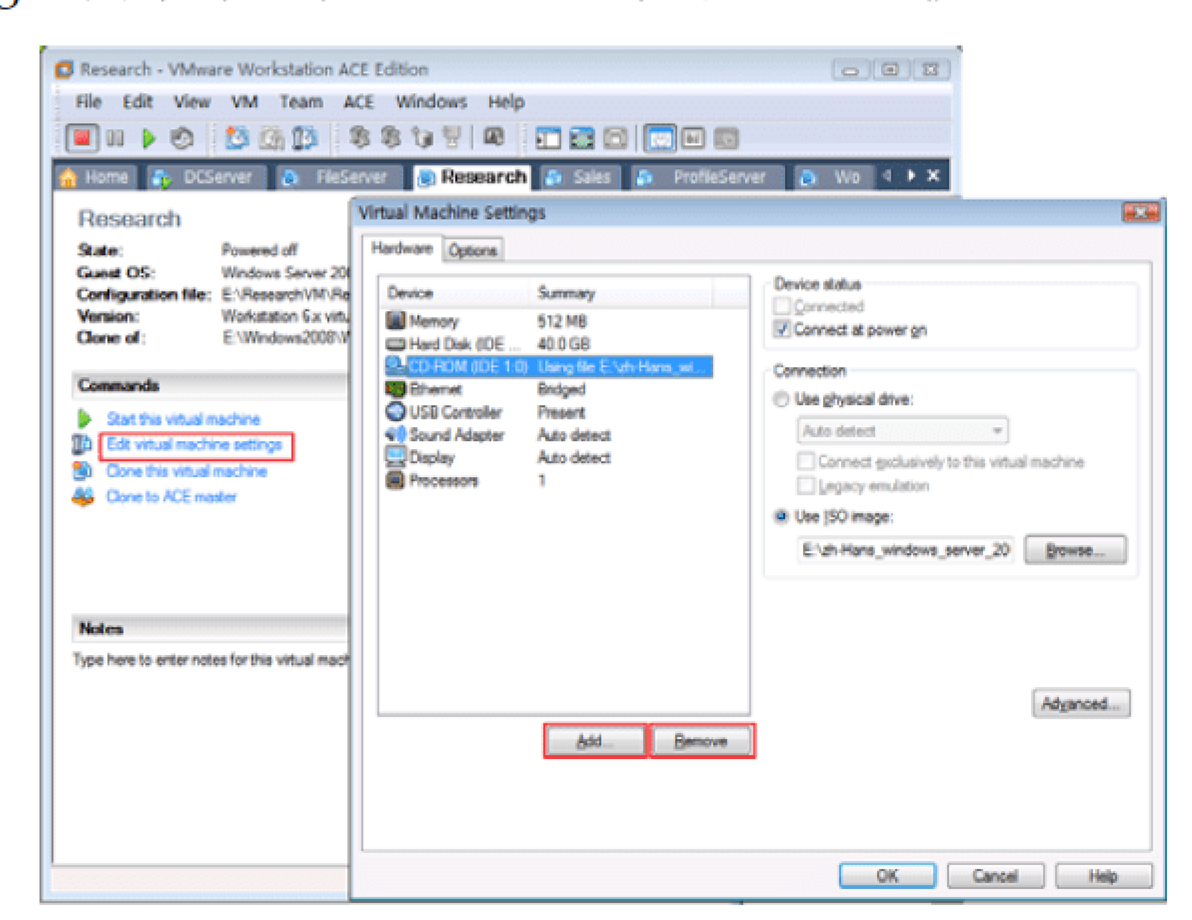


图 11-97 删除光驱

⑥　如图 11-97 所示，单击 Add 按钮。

⑦　如图 11-98 所示，在出现的 Hardware Type 界面中，选中 Hard Disk，单击 Next 按钮。

⑧　如图 11-99 所示，在出现的 Select a Disk 界面中，选中 Use an existing virtual disk 单选按钮，单击 Next 按钮。

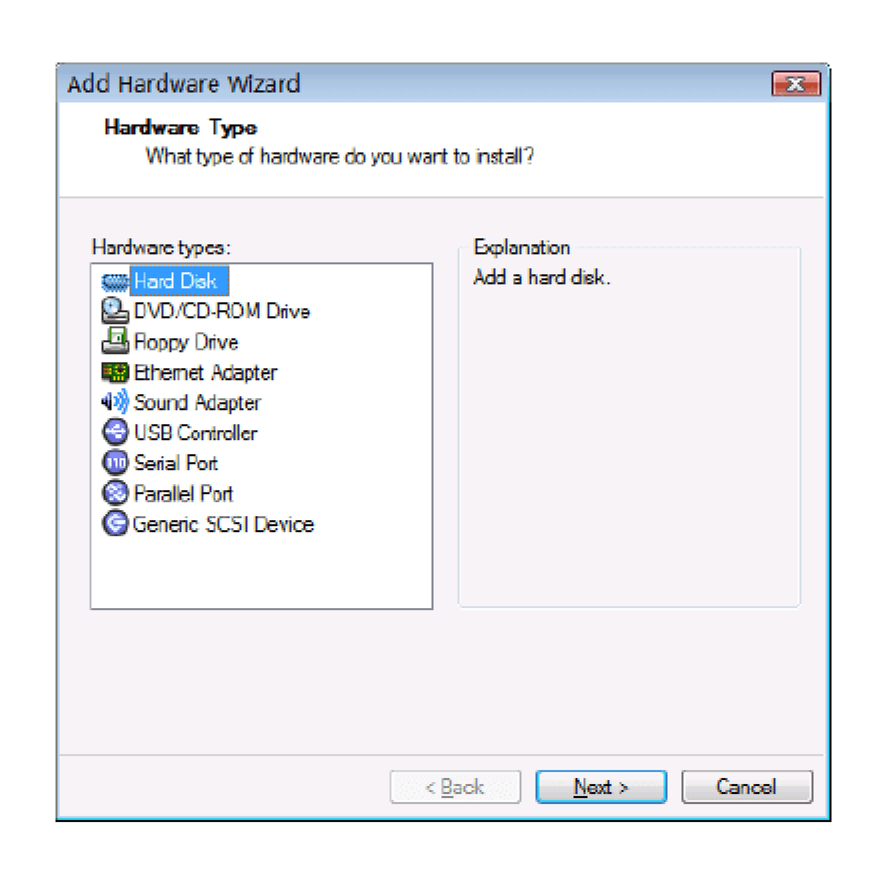


图 11-98　添加硬盘 1

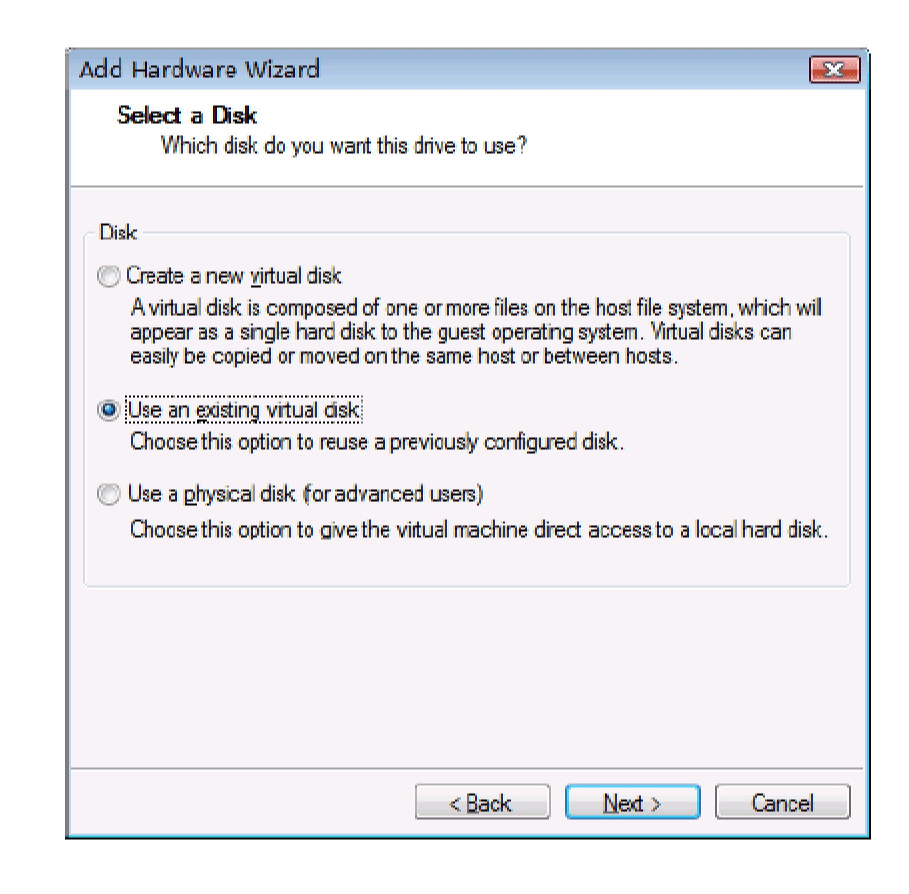


图 11-99　添加硬盘 2

⑨　如图 11-100 所示，在 Specify Disk File 界面中，单击 Browse 按钮，浏览到 FileServer 虚拟机所在的目录，选中 FirstDisk.vmdk，单击 Finish 按钮。

⑩　以同样的方法添加 NewDisk.vmdk 和 ThirdDisk.vmdk。

⑪　启动 Research。

⑫　如图 11-101 所示，打开服务器管理器，展开“存储”→“磁盘管理”节点。可以看到镜像卷和 RAID-5 卷提示“失败的重复”。

⑬　如图 11-101 所示，磁盘 1 还有提示。

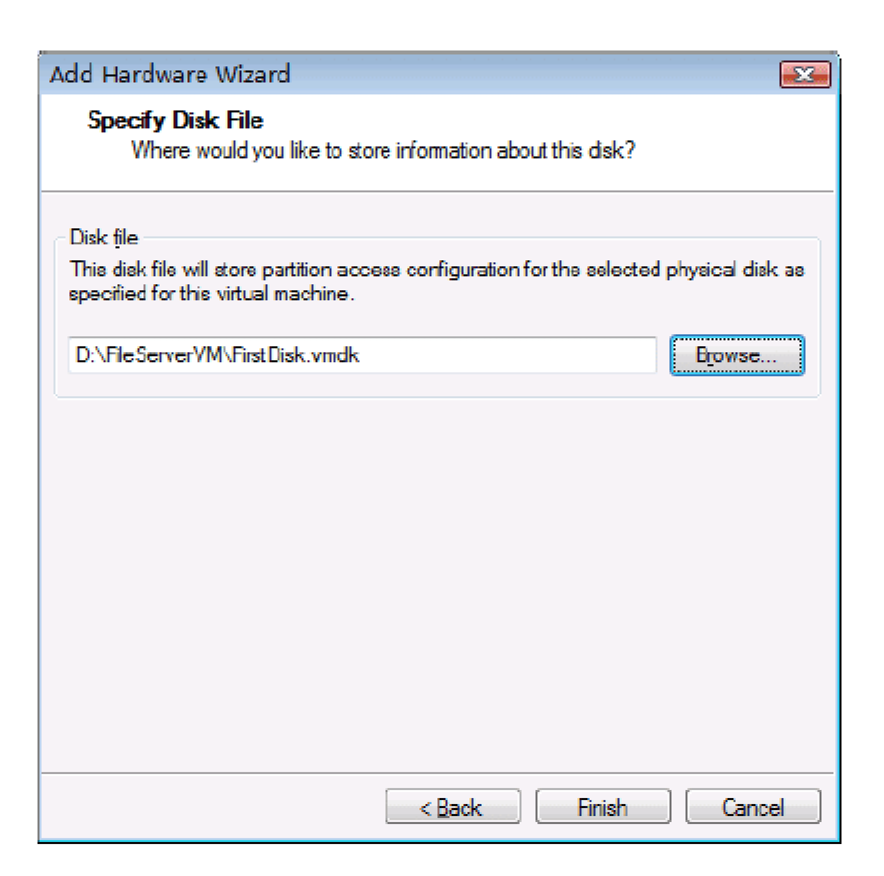


图 11-100　浏览到磁盘

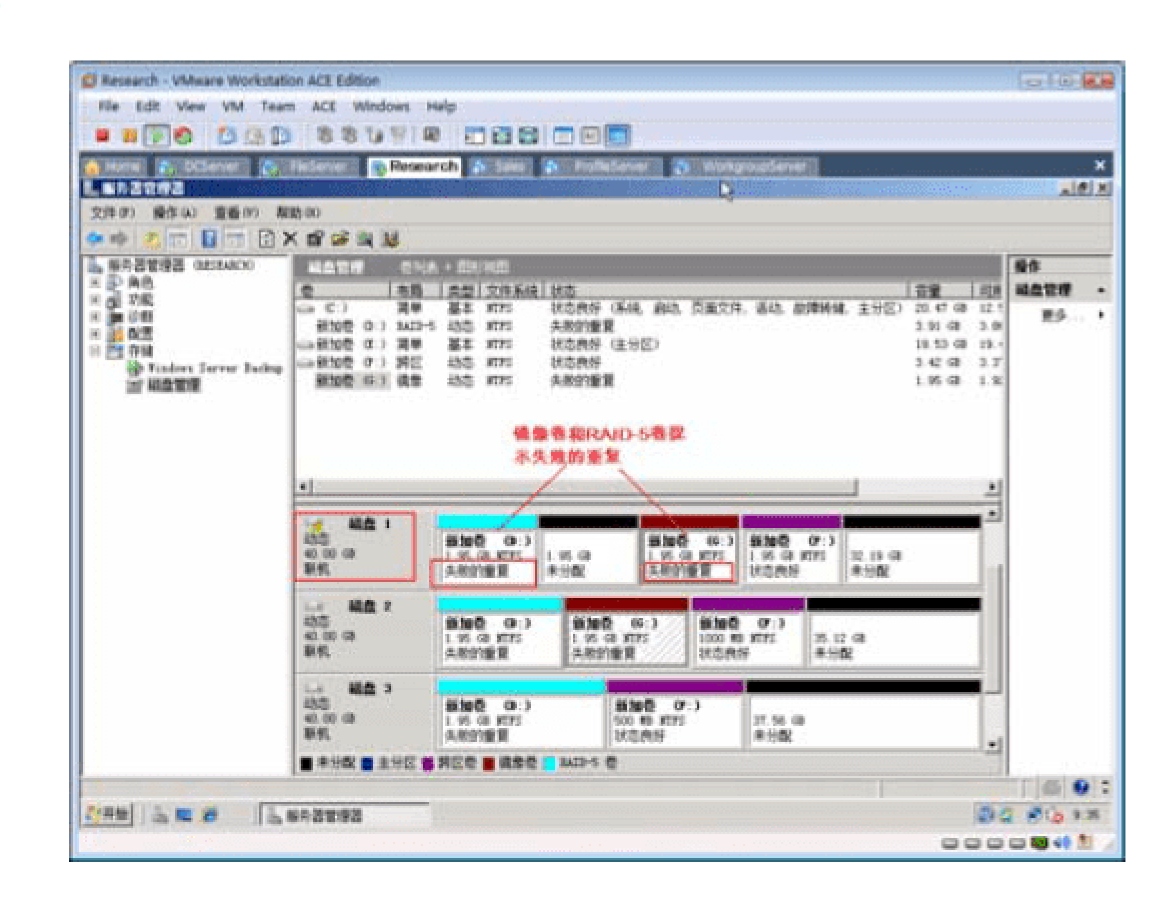


图 11-101　磁盘 1 未激活

⑭　如图 11-102 所示，右击磁盘 1，从弹出的快捷菜单中选择“重新激活磁盘”命令。

⑮　如图 11-103 所示，可以看到，重新激活过程，就是镜像卷和 RAID-5 同步的过程。

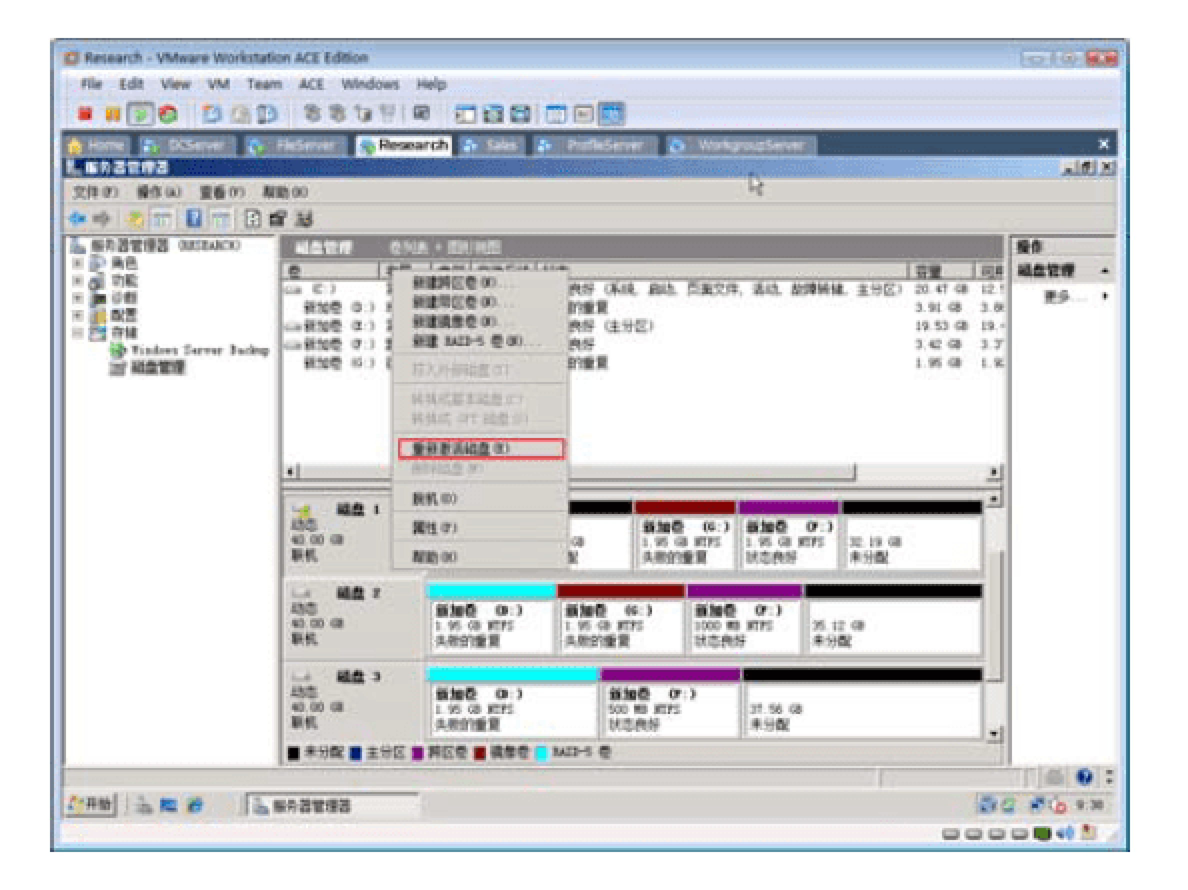


图 11-102　重新激活磁盘

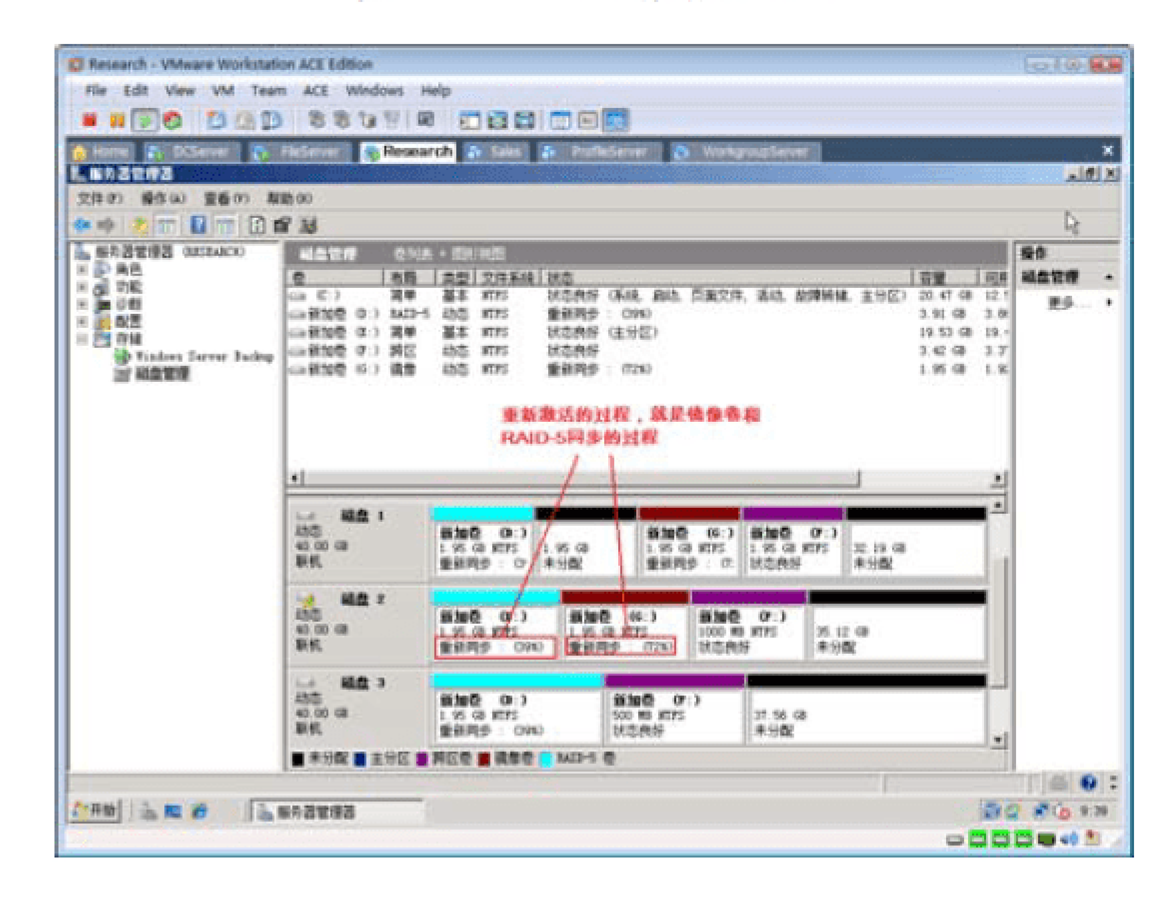


图 11-103　激活 RAID-5

第 12 章　终端服务器

可以在服务器上启用远程桌面来远程管理服务器，不需要购买许可证，但只能并发连接两个会话。

如果打算让更多的人使用服务器上的程序，需要在服务器上安装终端服务，连接的用户数量由终端服务授权服务器颁发的终端服务许可证数量决定。

配置终端服务器安全，允许一个用户有多个终端会话，将本地资源映射到远程桌面，在域环境中配置单一登录。

配置终端服务，发布 RemoteAPP，在客户端使用终端服务发布的应用程序。

客户机使用 DMZ 区网络中的终端服务网关访问内网的安装终端服务器和启用了远程桌面的服务器。这样客户端可以使用 SSL 协议访问到 DMZ 区的 TS 网关，TS 网关再使用 RDP 协议访问内网的服务器。

TS Session Broke 是 Windows Server 2008 中的新特性，是用于终端服务的 Microsoft Network Load Balancing 更简单的一个替代产品，终端服务器不局限于一个网段。

关键词

- 使用远程桌面管理服务器
- 启用 Windows Server Core 的远程桌面
- 将本地资源映射到远程服务器
- 在域环境中配置远程桌面的单一登录
- 配置终端服务器安全
- 终端服务
- 安装并激活终端服务授权
- 安装终端服务
- 配置和使用终端服务器的 RemoteApp
- 配置终端服务网关
- 使用终端服务网关连接到内网的终端服务
- 配置终端服务器场实现终端服务负载均衡

12.1　本 章 环 境

本章的实战环境如图 12-1 所示。

目标

- 学会在服务器上启用远程桌面。
- 授权用户使用远程桌面连接到服务器。
- 能够在远程桌面配置客户端。
- 能够配置远程桌面属性。
- 能够在服务器上安装终端服务器授权。
- 能够激活终端服务授权。
- 学会在服务器上安装终端服务。
- 配置并使用终端服务器的 RemoteApp。
- 能够配置终端服务网关。
- 能够使用终端服务网关连接到终端服务和远程桌面。
- 能够配置终端服务器场实现终端服务负载均衡。

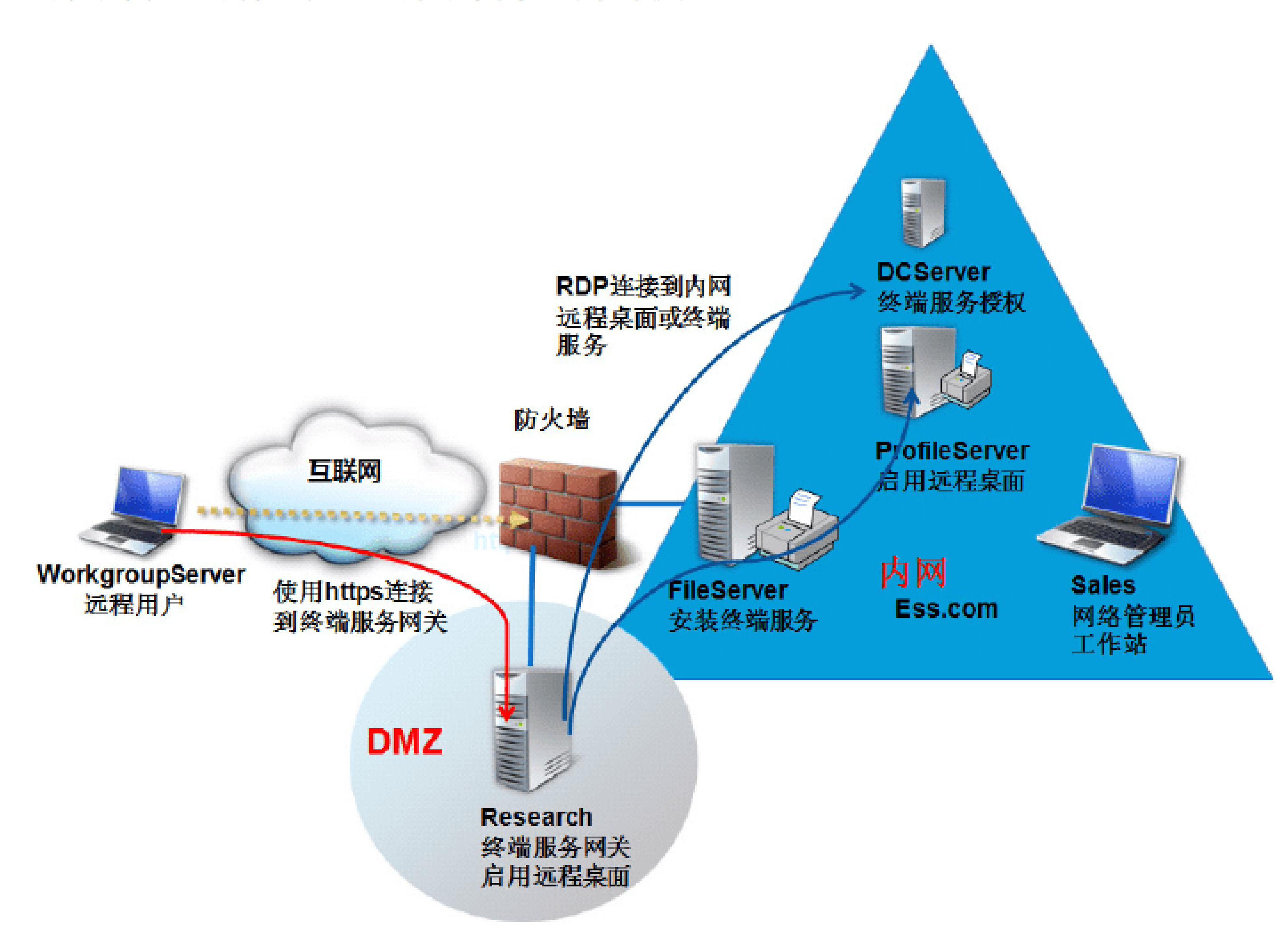


图 12-1　实战环境

操作系统

- DCServer 是 Ess.com 域中的域控制器，安装 Windows Server 2008 企业版操作系统。
- FileServer 是 Ess.com 域中的应用程序服务器，安装 Windows Server 2008 企业版操作系统。
- Research 是 Ess.com 域中的成员，安装 Windows Server 2008 企业版操作系统。
- ProfileServer 是 Ess.com 域中的文件服务器，安装 Windows Server Core 系统。
- WorkgroupServer 是工作组中的计算机，安装 Windows Server 2008 企业版操作系统。

网络环境

- Research 计算机处于 DMZ 区。
- WorkgroupServer 处于 Internet。
- FileServer、Sales、ProfileServer 和 DC 处于内网。

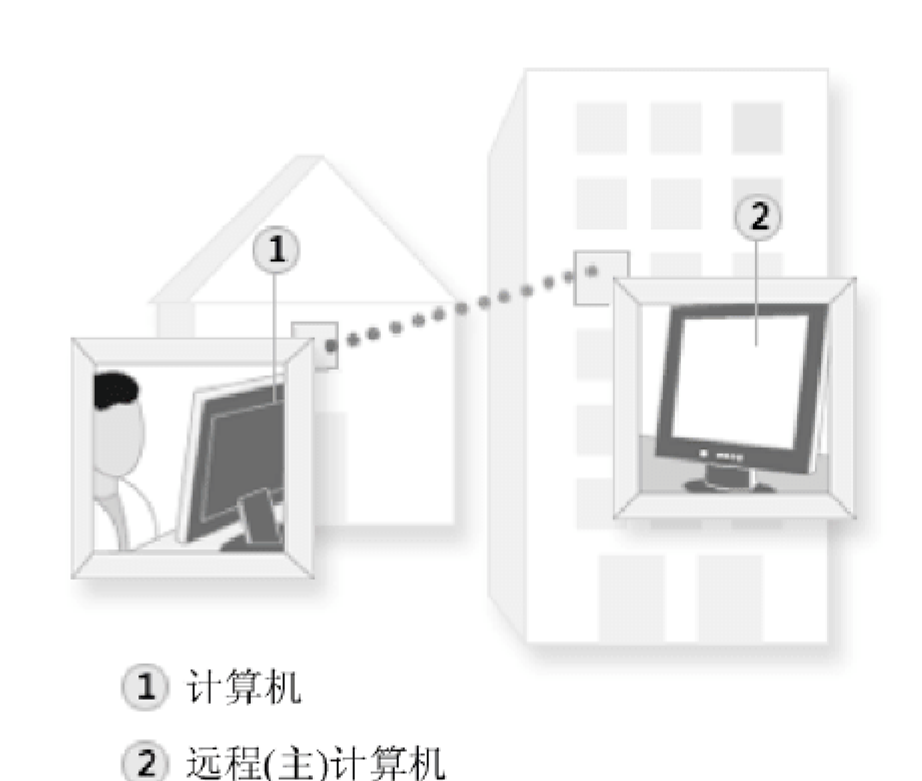
要求

- 网络管理员需要使用 Sales 计算机远程管理 Research 服务器。
- 网络管理员需要使用 Sales 计算机远程管理 Sales 服务器。
- FileServer 服务器安装有公司的测试软件，很多用户需要使用 FileServer 上的软件。
- 在 Research 服务器上安装终端服务网关。

12.2 使用远程桌面管理服务器

使用远程桌面管理(Remote Desktop for Administration)，可以从一个位置来管理一台或多台远程计算机。在一个大规模的组织中，可以使用远程管理来集中化地管理多台位于不同建筑物甚至位于不同城市的计算机；而在一个小规模的组织中，可以利用远程管理来管理位于邻近办公室中的单台服务器。

远程桌面管理通过使用 RDP(Remote Desktop Protocol，远程桌面协议)来实现从位于一个位置的计算机访问位于另一个位置的服务器的功能。RDP 将用户接口传输到客户端会话，还可将键盘和鼠标的单击从客户端传输到服务器。远程桌面不需要购买连接许可，最多可同时创建两个远程连接。所有登录的会话都独立于其他客户端会话和服务器控制台会话。如图 12-2 所示，当我们使用远程桌面管理远程登录到服务器时，就如同在本地登录一样。



两台计算机之间的远程桌面连接

图 12-2 远程桌面

12.2.1 使用远程桌面管理的好处

远程桌面管理是一项方便、高效的服务，通过远程桌面管理可以极大降低与远程管理有关的费用。例如，我们可以通过远程桌面管理允许多个管理员管理多台远程服务器。

远程桌面管理允许我们启动服务器上的一个新的远程会话，或者远程接收在一台服务器上的控制台会话。然而，同一时刻在一台服务器上只能运行一个控制台会话。例如，当你远程登录一个控制台时，已有一个管理员登录到该控制台，那么你将无法登录到该控制台。

使用远程桌面管理可以提供以下一些好处。

- 支持对 Windows Server 2008 的完全管理。使用远程桌面连接，系统管理员可以从运行 Windows Server 2008 或以前版本的 Windows 操作系统(Windows 95/98、Windows 2000、Windows XP 或 Vista)的计算机上来完全管理运行 Windows Server 2008 的计算机。
- 从任意位置访问服务器。使用远程桌面管理，我们可以在世界上的任何地点，通过广域网(WAN)、虚拟专用网络(VPN)或拨号连接来访问远程服务器。
- 访问配置设置。使用远程桌面管理，可以远程访问服务器的大多数的配置设置，包括控制面板。使用远程桌面会话，我们可以访问 MMC、Active Directory、Microsoft 系统管理服务器、网络配置工具和大多数的其他管理工具。
- 诊断故障和测试解决方案。使用远程桌面管理，我们可以快速地诊断客户计算机和服务器的故障，并可以测试所采取的解决方案。
- 执行耗时的批量管理工作。使用远程桌面管理，我们可以远程执行耗时的批处理的管理工作，例如磁带备份。
- 远程更新服务器操作系统和应用程序。通过远程桌面管理我们可以远程地更新服务器应用程序。

12.2.2 启用远程桌面

系统管理员可以使用远程桌面来执行远程管理任务。例如：可以在远程服务器上安装软件或服务包。在用远程桌面管理远程服务器之前，远程服务器必须在本地端启用远程桌面。

1. 在服务器上启用远程桌面

① 右击桌面上的“计算机”图标，从弹出的快捷菜单中选择“属性”命令，在打开的“系统”对话框中单击“远程设置”选项。

② 如图 12-3 所示，在“系统属性”对话框的“远程”选项卡中，选中“允许运行任意版本远程桌面的计算机连接”单选按钮。

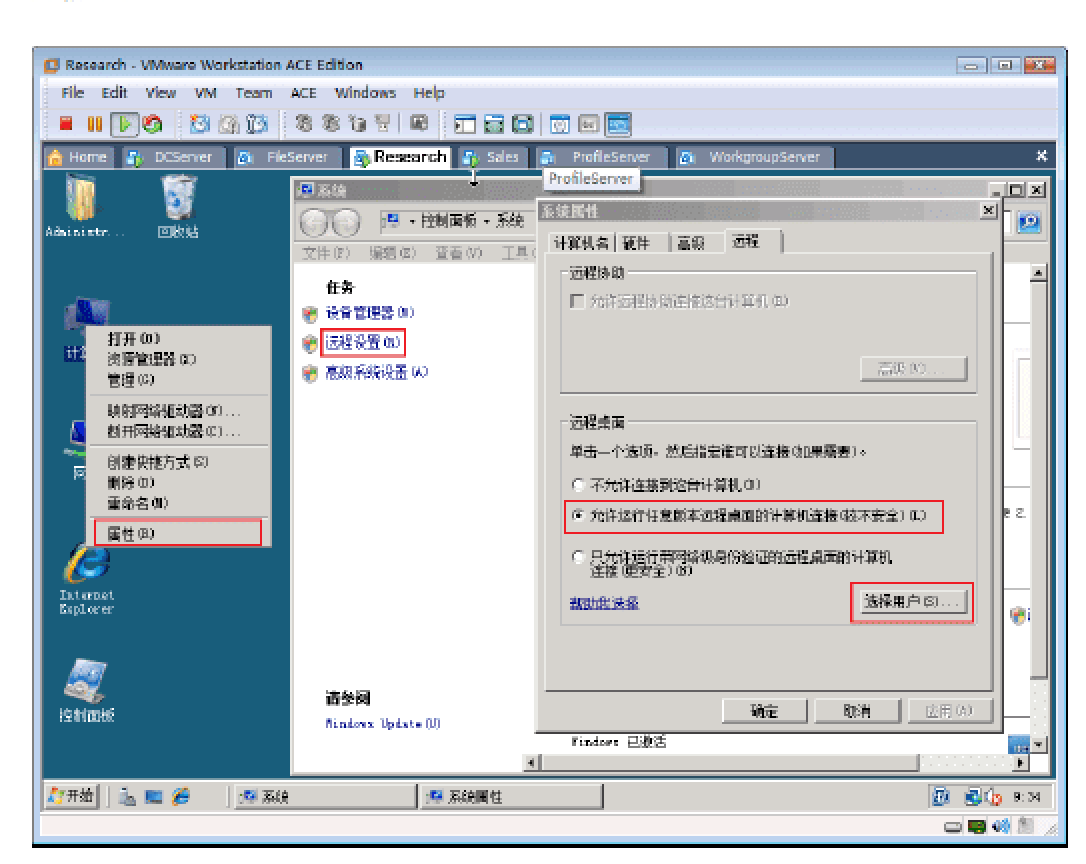


图 12-3 启用远程桌面

③　单击“选择用户”按钮。

④　如图 12-4 所示，在出现的“远程桌面用户”对话框中，单击“添加”按钮。

⑤　如图 12-4 所示，在出现的“选择用户或组”对话框中，输入 han，单击“检查名称”按钮，单击“确定”按钮。

⑥　如图 12-5 所示，等同于在 Remote Desktop Users 组添加 han 用户。

注意：可以允许使用运行带网络级身份验证 (NLA) 的远程桌面或 TS RemoteApp 版本计算机的人连接到你的计算机。如果你知道将要连接到你计算机的人在其计算机上运行 Windows Vista，这是最安全的选择。(在 Windows Vista 中，远程桌面使用 NLA)

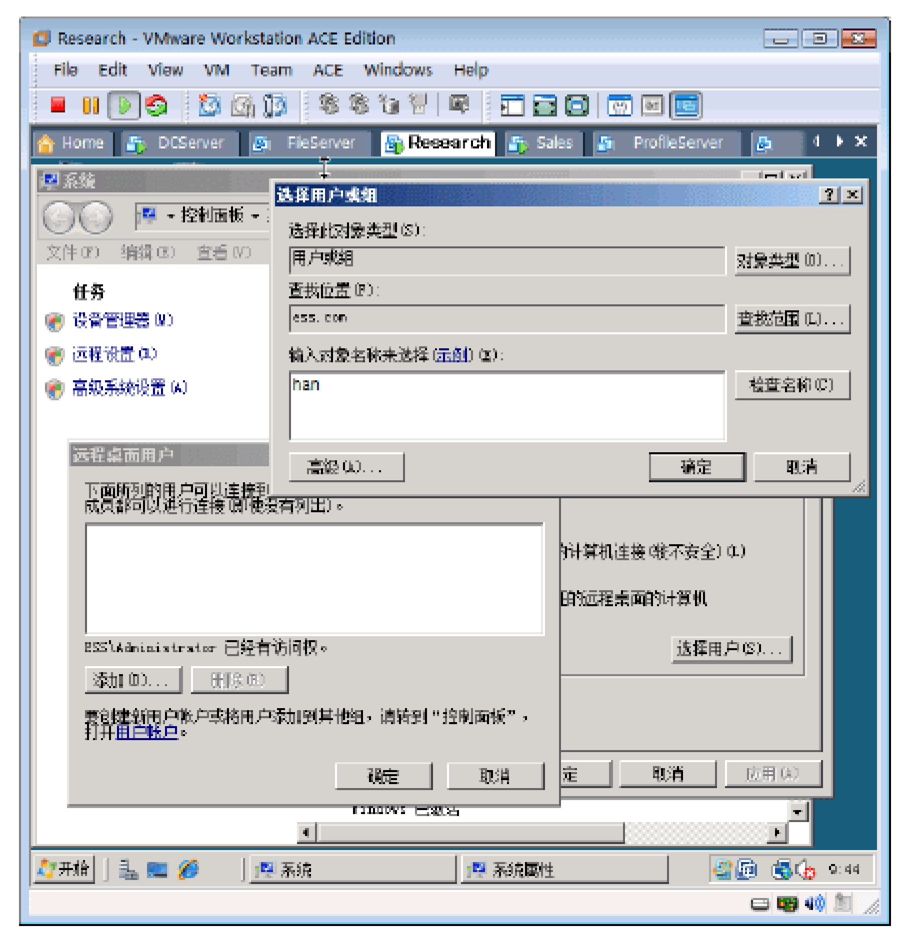


图 12-4　添加用户到 Remote Desktop Users 组

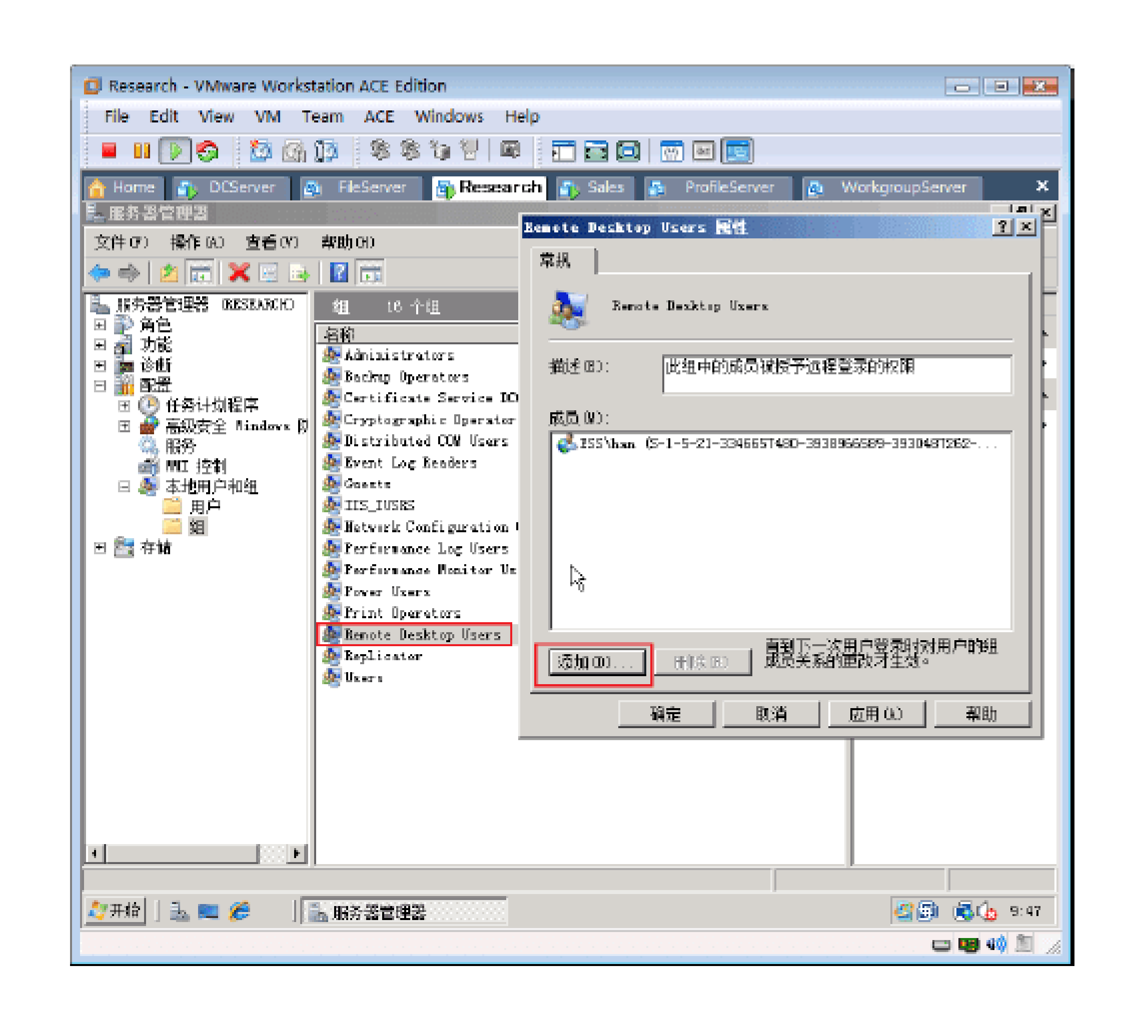


图 12-5　查看 Remote Desktop Users 组成员

2. 什么是网络级身份验证

网络级身份验证 (NLA) 是一种新的身份验证方法，在用户建立所有远程桌面连接之前完成用户身份验证，并出现登录屏幕。 这是最安全的身份验证方法，有助于保护远程计算机避免黑客或恶意软件的攻击。NLA 的优点如下。

- 最初需要较少的远程计算机资源。验证用户之前，远程计算机使用有限的资源，而不是像以前版本那样启动所有远程桌面连接。
- 可以通过减少拒绝服务攻击(试图限制或阻止访问 Internet)来帮助提供更高的安全。
- 使用远程计算机身份验证，从而帮助用户避免连接到设置为恶意目的的远程计算机。

12.2.3　启用 Windows Server Core 远程桌面

①　以域管理员身份登录到安装 Windows Server Core 操作系统的 ProfileServer，如图 12-6 所示。

②　在命令提示符下，输入 cd \，按 Enter 键。

③　输入 cd windows\system32，按 Enter 键。

④　输入 cscript SCregEdit.wsf /Ar 0，按 Enter 键。

⑤　输入 netsh firewall add portopening tcp 3389 Remote-Desktop，按 Enter 键。

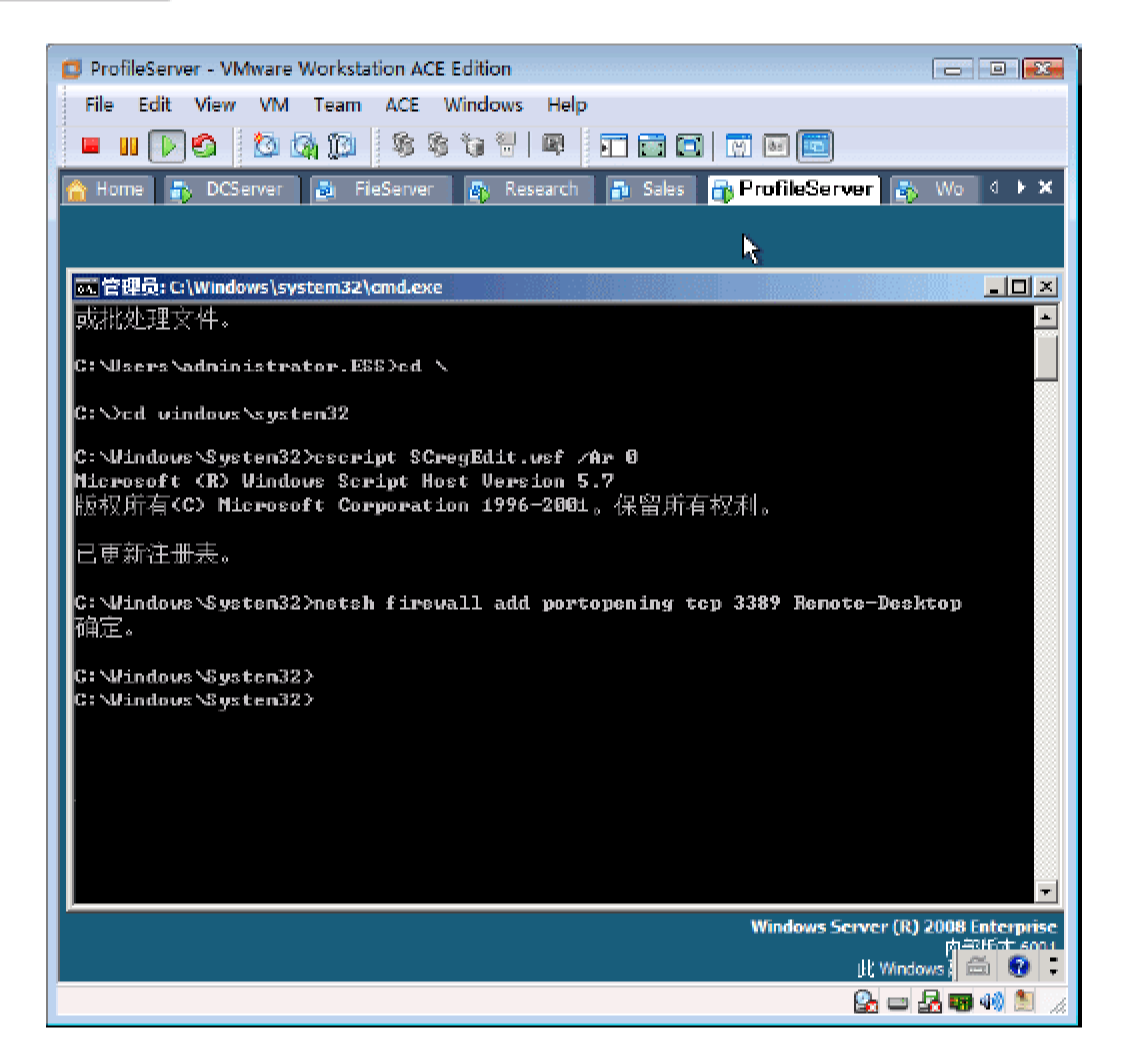


图 12-6　启用远程桌面打开防火墙端口

12.3　使用远程桌面连接连接到其他计算机

使用远程桌面连接，可以从一台运行 Windows 的计算机访问另一台运行 Windows 的计算机，条件是两台计算机连接到相同网络或连接到 Internet。例如，可以在家中的计算机使用所有工作的计算机的程序、文件及网络资源，就像坐在工作场所的计算机前一样。

若要连接到远程计算机，该计算机必须为开启状态，必须具有网络连接，远程桌面必须可用，必须能够通过网络访问该远程计算机(可通过 Internet 实现)，还必须具有连接权限。若要获取连接权限，你必须位于用户列表中。下面介绍如何将名称添加到该列表中。



注意：不能使用远程桌面连接连接到运行 Windows Vista Starter、Windows Vista Home Basic、Windows Vista Home Basic N 或 Windows Vista Home Premium 的计算机，只能从这些版本的 Windows Vista 创建接出连接。无法使用远程桌面连接连接到运行 Windows XP Home Edition 的计算机。

12.3.1　连接到服务器的远程桌面

在 Sales 计算机上，连接到 Research 的远程桌面。

① 如图 12-7 所示，选择“开始”→“程序”→“附件”→“远程桌面连接”命令，或选择“开始”→“运行”命令，在出现的“运行”对话框中输入 mstsc，单击“确定”按钮。

② 如图 12-8 所示，在“远程桌面连接”对话框中，输入 research，单击“连接”按钮。

③ 如图 12-8 所示，在出现的“输入您的凭据”界面中，输入账号和密码，选中“记住我的凭据”复选框，单击“确定”按钮。

④ 如图 12-9 所示，远程桌面连接成功，可以看到 Research 计算机上的桌面。

⑤ 如图 12-10 所示，选择“控制面板”→“用户帐户”→“管理网络密码”命令，可以看到已经自动存储了访问 Research 服务器的账号和密码。

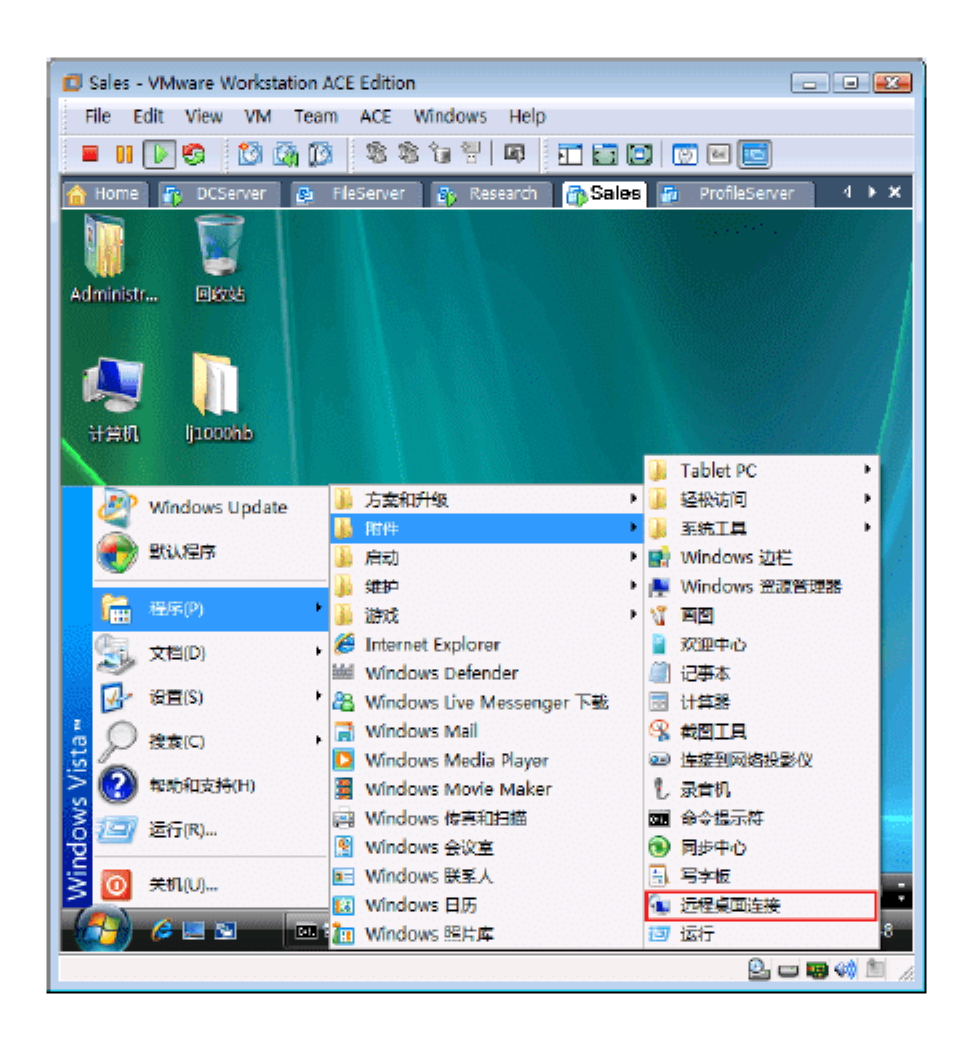


图 12-7　打开远程桌面客户端

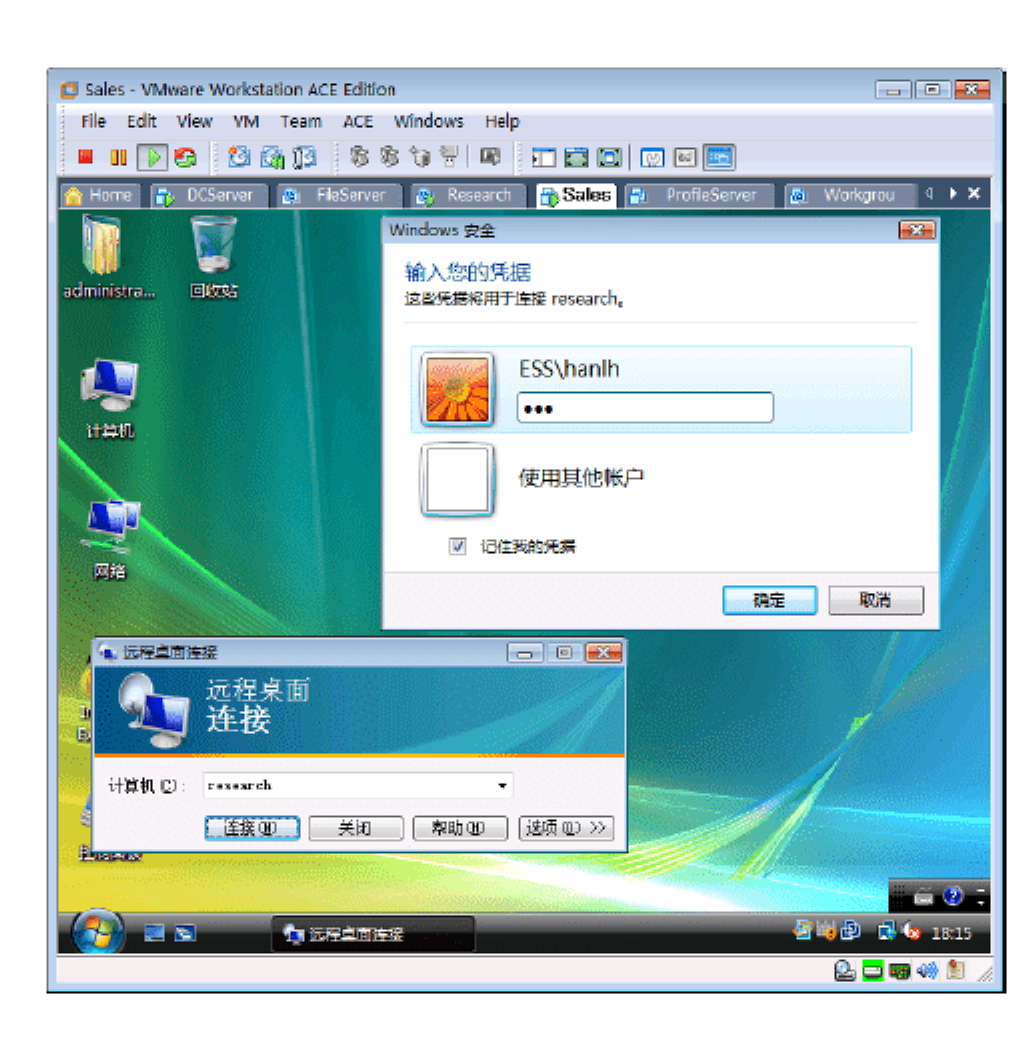


图 12-8　输入账号和密码

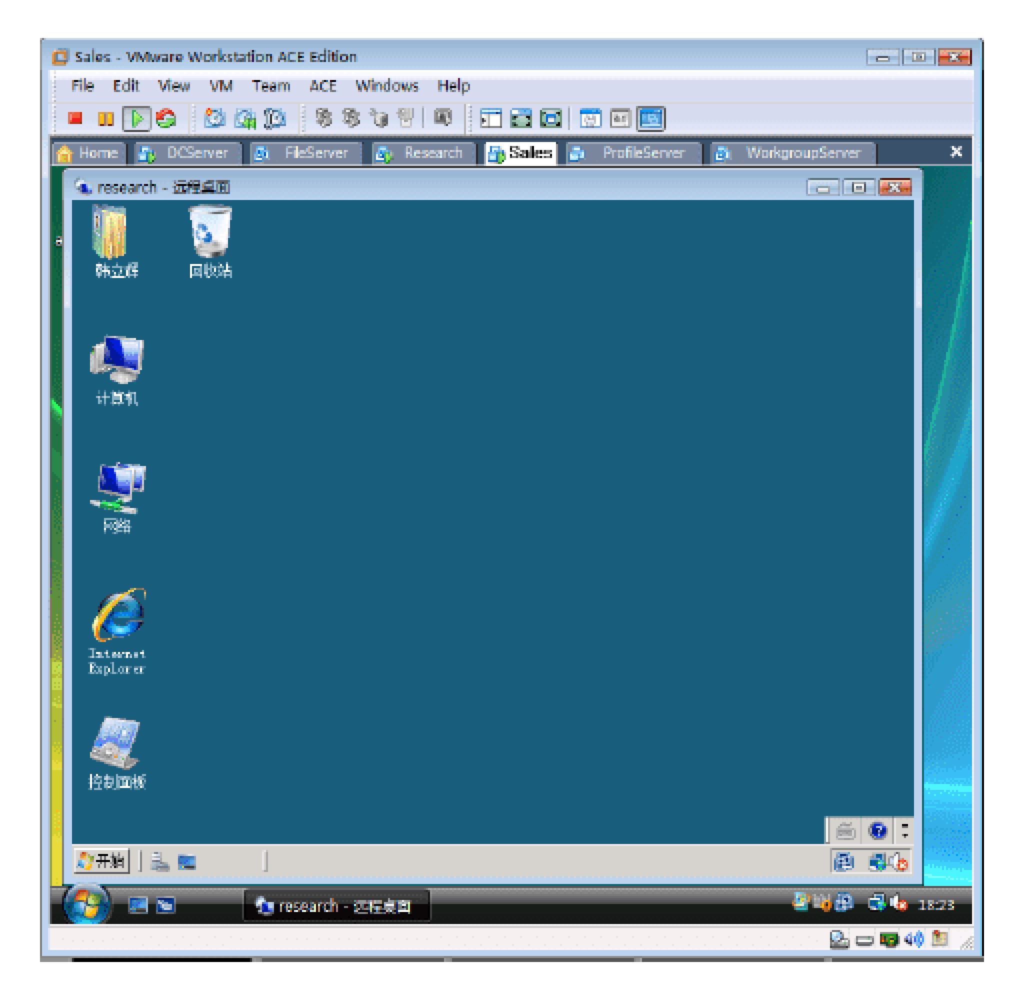


图 12-9　远程桌面

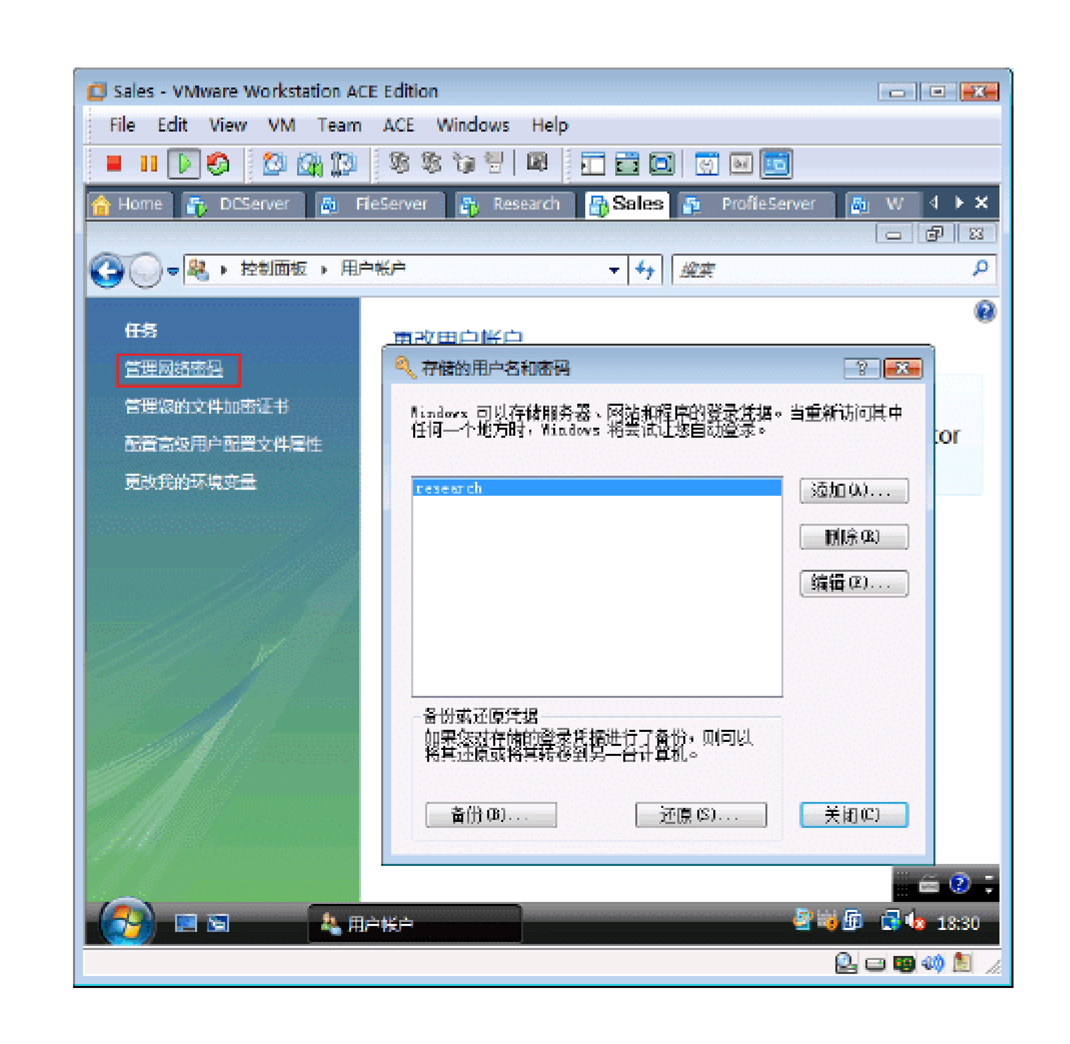


图 12-10　存储的账号和密码

12.3.2　将资源映射到远程服务器

用户在 Sales 计算机上办公，在使用远程桌面管理 Research 计算机时，需要用到 Sales 计算机磁盘上的一些文件。

将本地磁盘映射到远程服务器

① 如图 12-11 所示，选择“开始”→“注销”命令，结束远程桌面连接。

② 如图 12-12 所示，打开远程桌面客户端，单击“选项”按钮。

③ 如图 12-13 所示，在“本地资源”选项卡中，可以看到本地打印机，剪切板默认能够在远程会话中使用。

④ 单击“详细信息”按钮，在出现的对话框中选中驱动器 C、D 和“稍后连接的驱动器”以及“支

持的即插即用”设备，如图 12-14 所示。单击“确定”按钮。

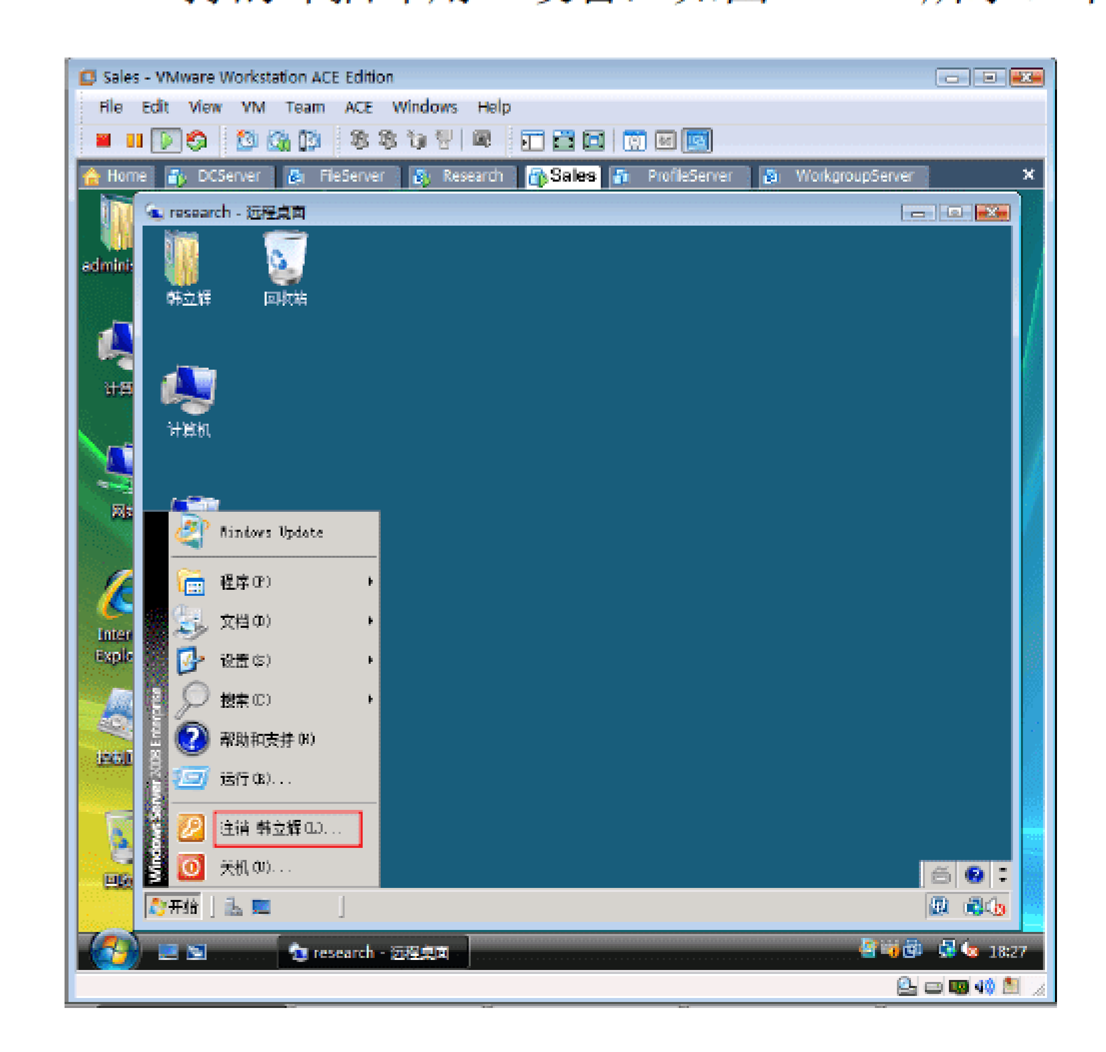


图 12-11　注销远程桌面登录

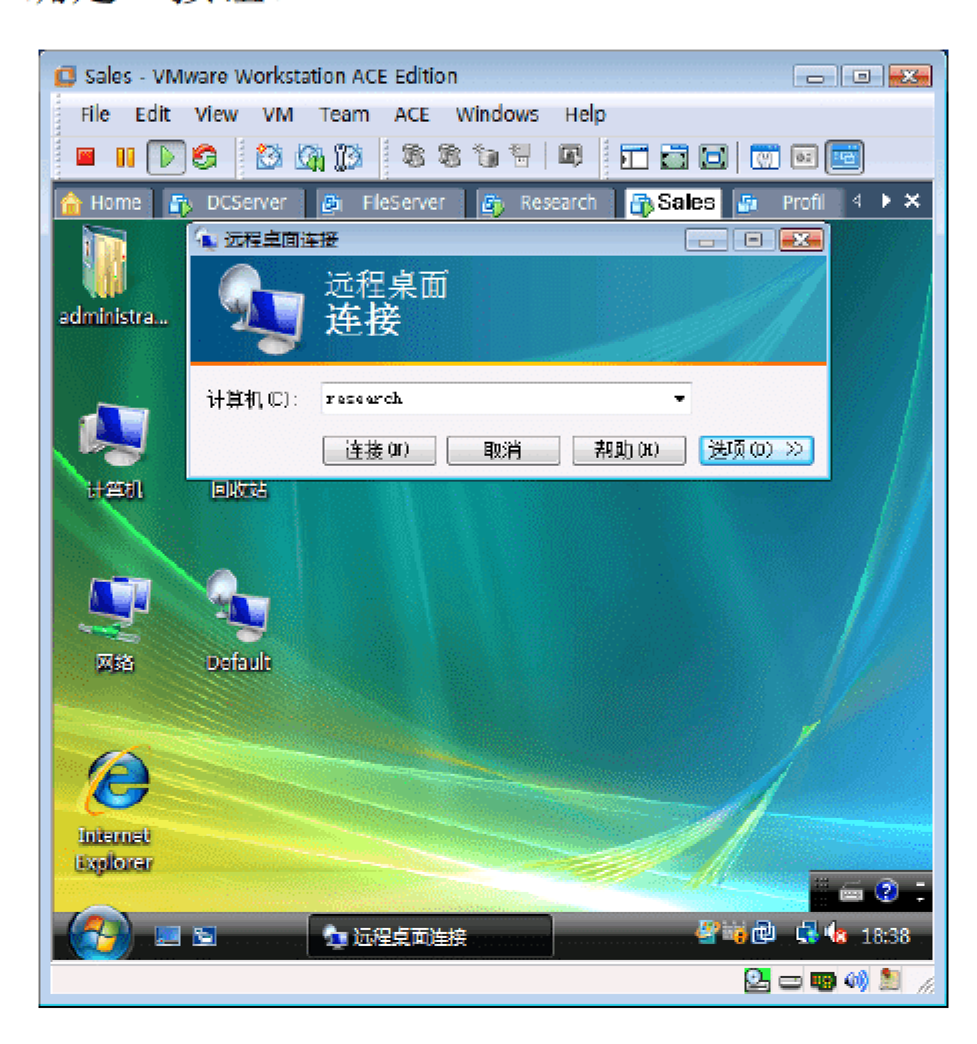


图 12-12　打开远程桌面客户端选项

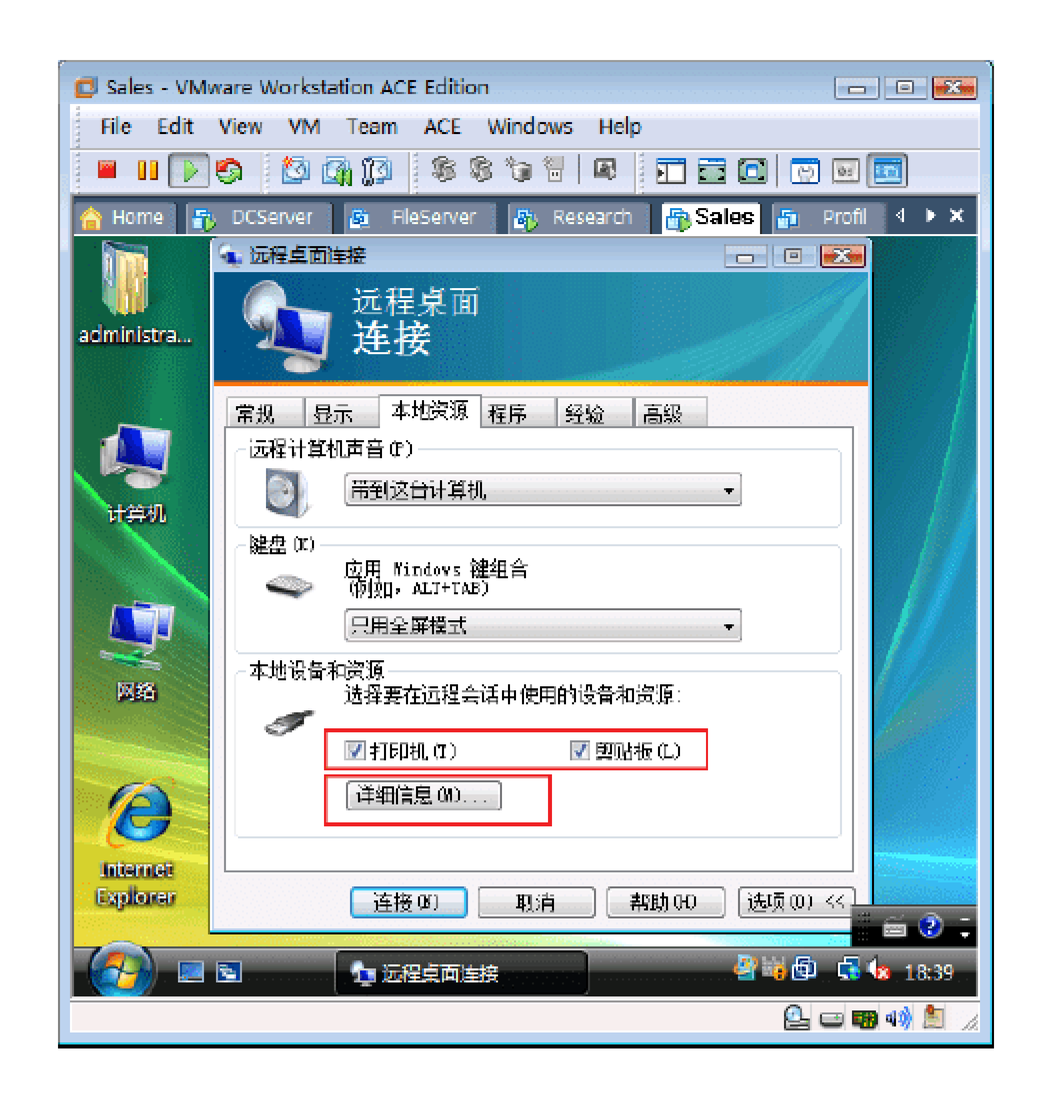


图 12-13　将本地资源映射到远程服务器

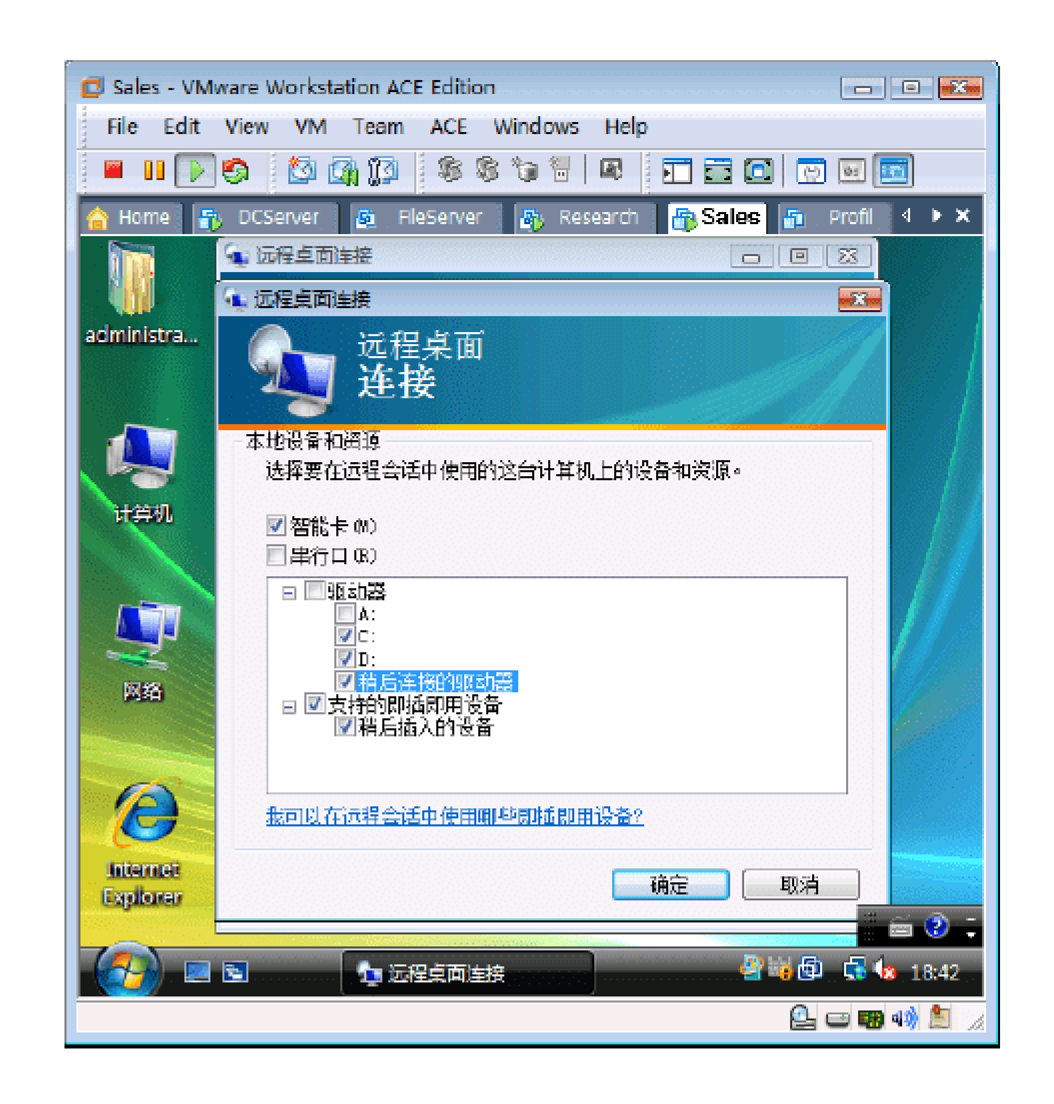


图 12-14　选择映射的驱动器

⑤　如图 12-15 所示，在出现的提示框中，选中“请不要再提示我连接到此计算机”复选框，单击“是”按钮。

⑥　如图 12-16 所示，登录成功后单击远程桌面中的计算机，可以看到映射到的 Sales 计算机上的 C 盘和 D 盘。

⑦　如图 12-17 所示，将 U 盘插入计算机，选择 VM→Removable Devices→USB Devices→SIS Removable Disk 命令，将 U 盘的控制权交给 Sales 计算机。

⑧　如图 12-18 所示，可以看到，在 Sales 本地刚刚插入的 U 盘，在远程桌面就能立刻发现并能使用。

⑨　如图 12-19 所示，选择远程桌面中的“开始”→“设置”→“打印机”命令，可以看到 Sales 上的打印机在远程桌面可用，这样就可以将远程桌面的打印作业发送到 Sales 计算机上的打印设备。

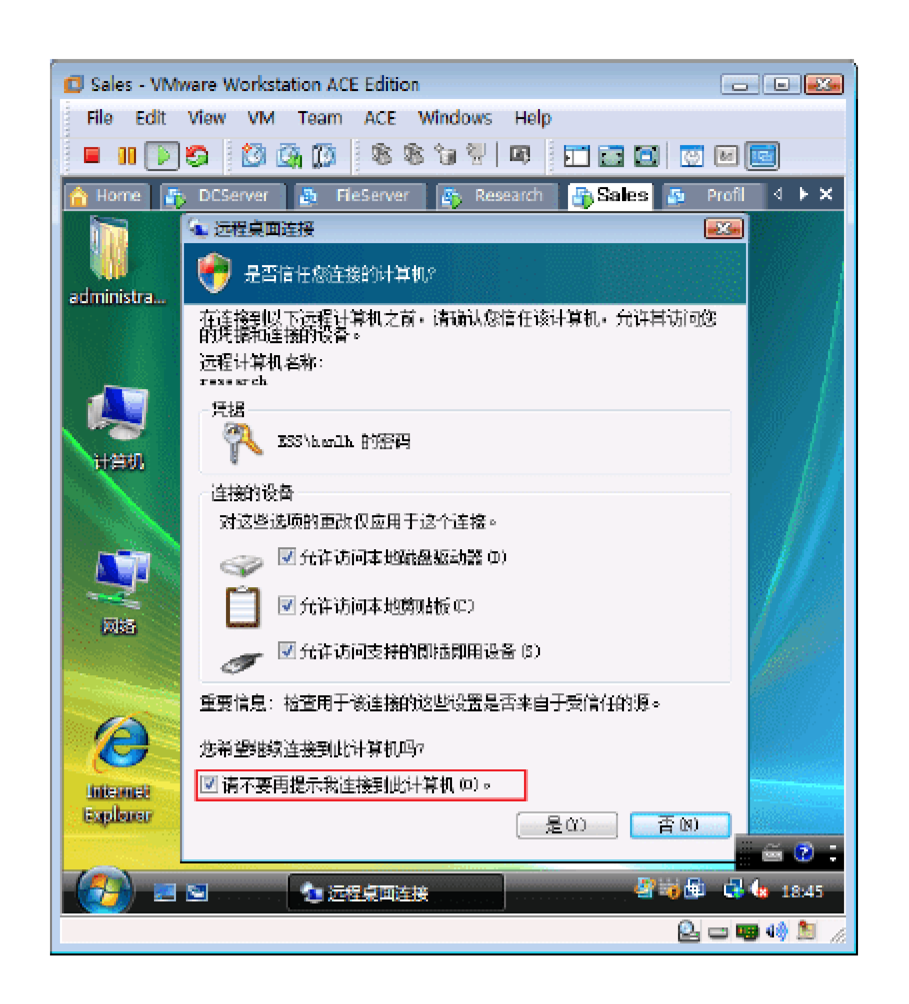


图 12-15　出现安全提示

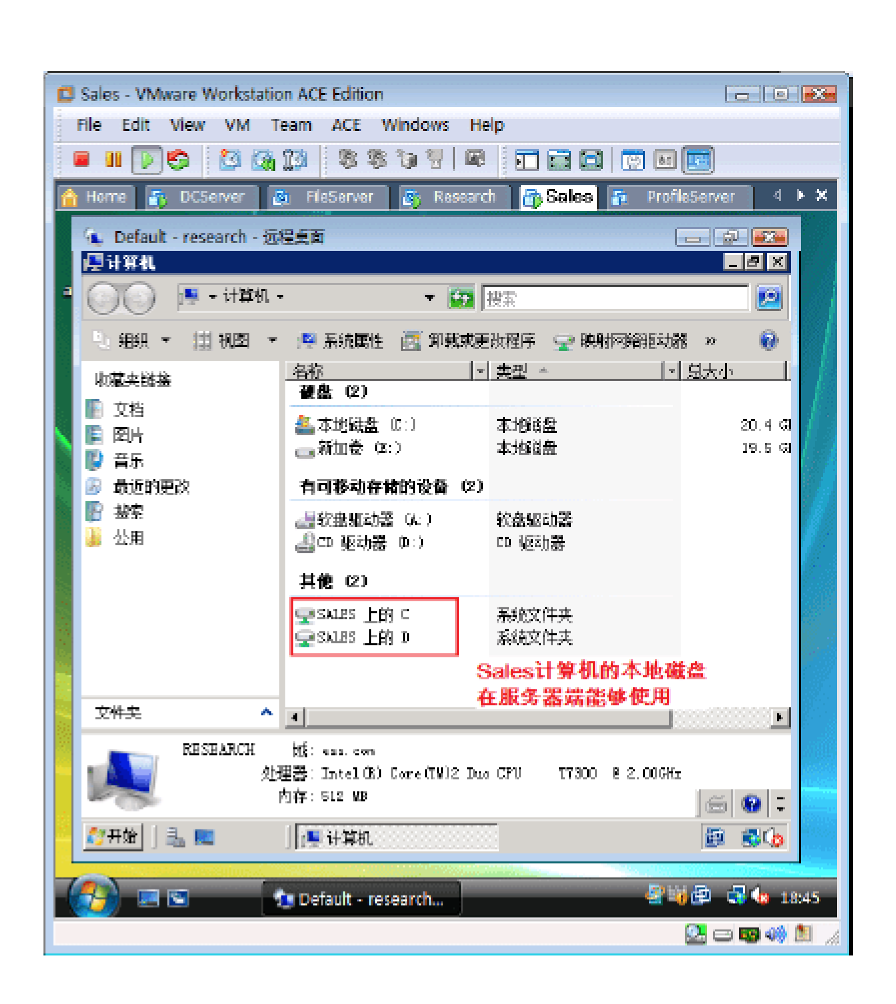


图 12-16　映射的本地资源

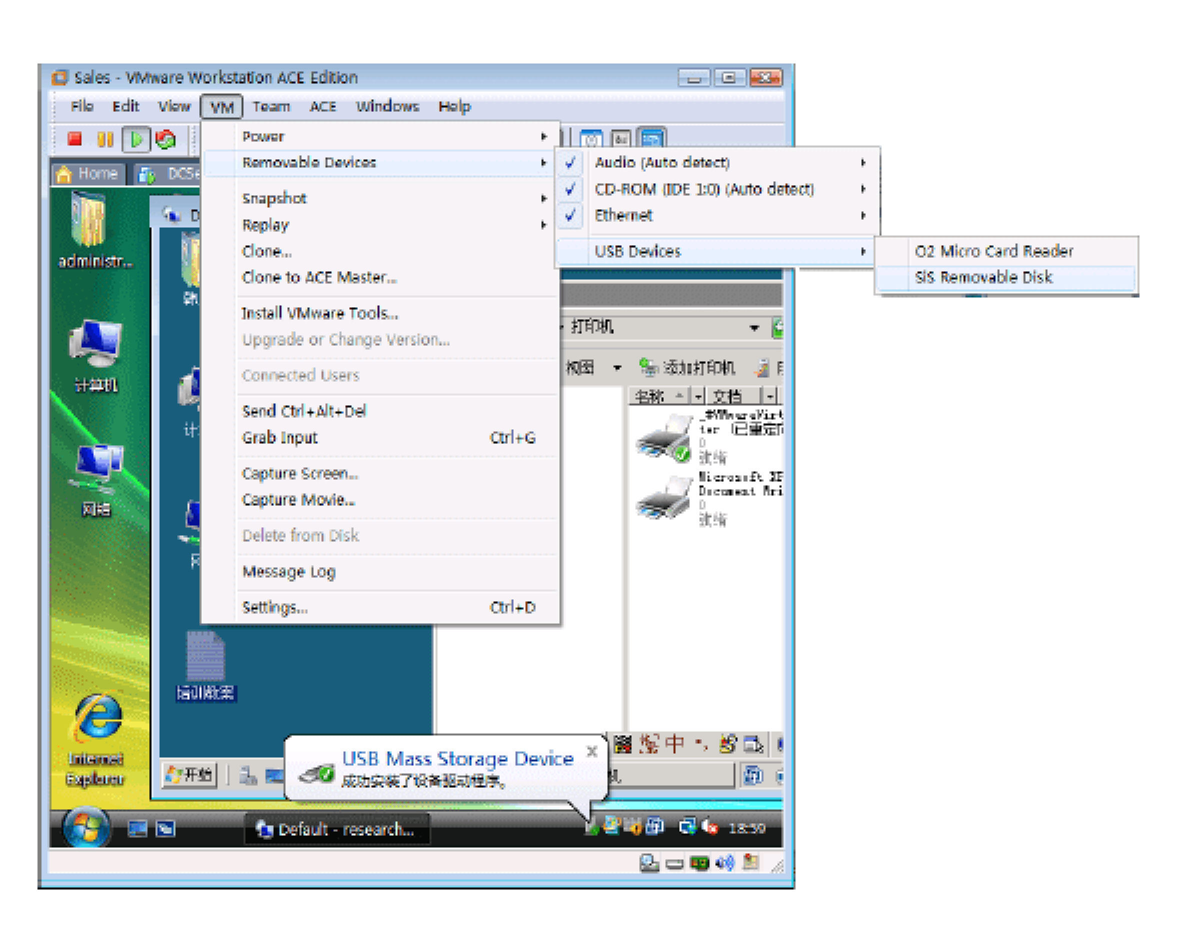


图 12-17　让虚拟机控制 USB 接口

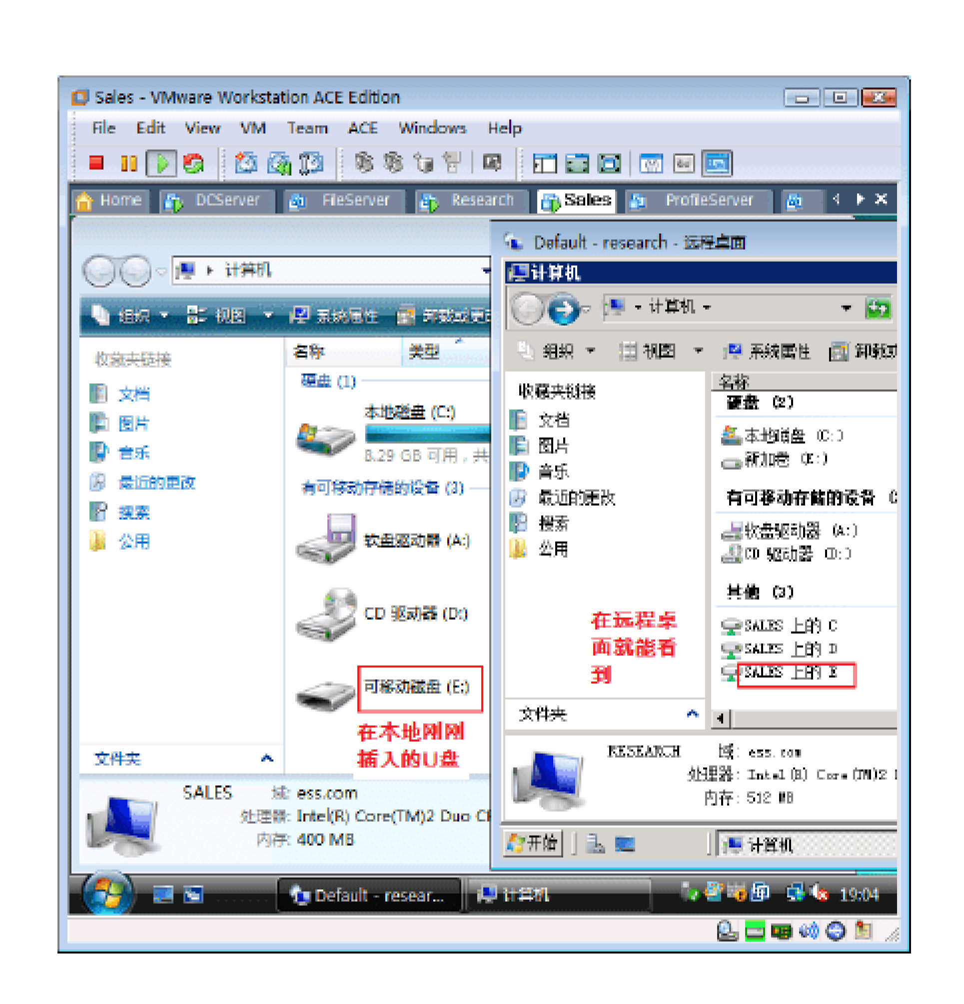


图 12-18　映射的本地 U 盘

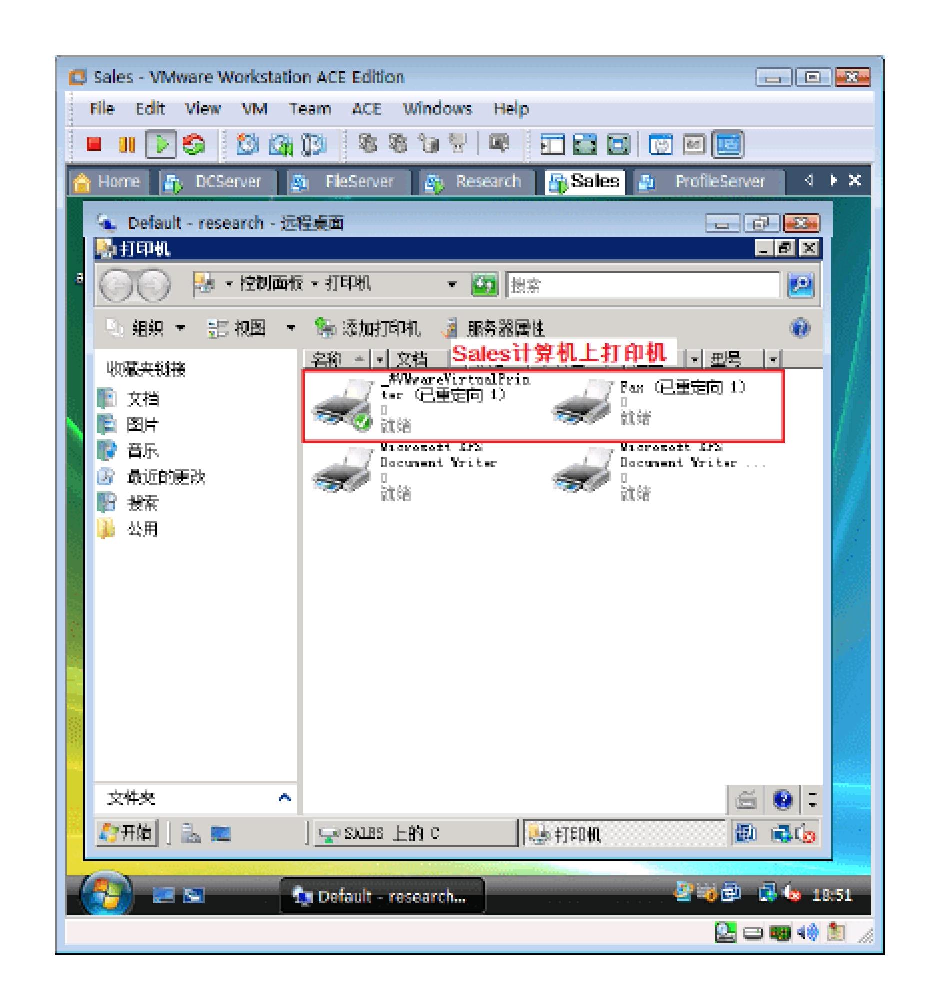


图 12-19　映射的本地打印机

⑩ 如图 12-20 所示，右击远程桌面上的一个文件，从弹出的快捷菜单中选择“复制”命令。

⑪ 如图 12-21 所示，右击 Sales 计算机的桌面，从弹出的快捷菜单中选择“粘贴”命令。这样可以将远程桌面的文件直接复制、粘贴到本地计算机。

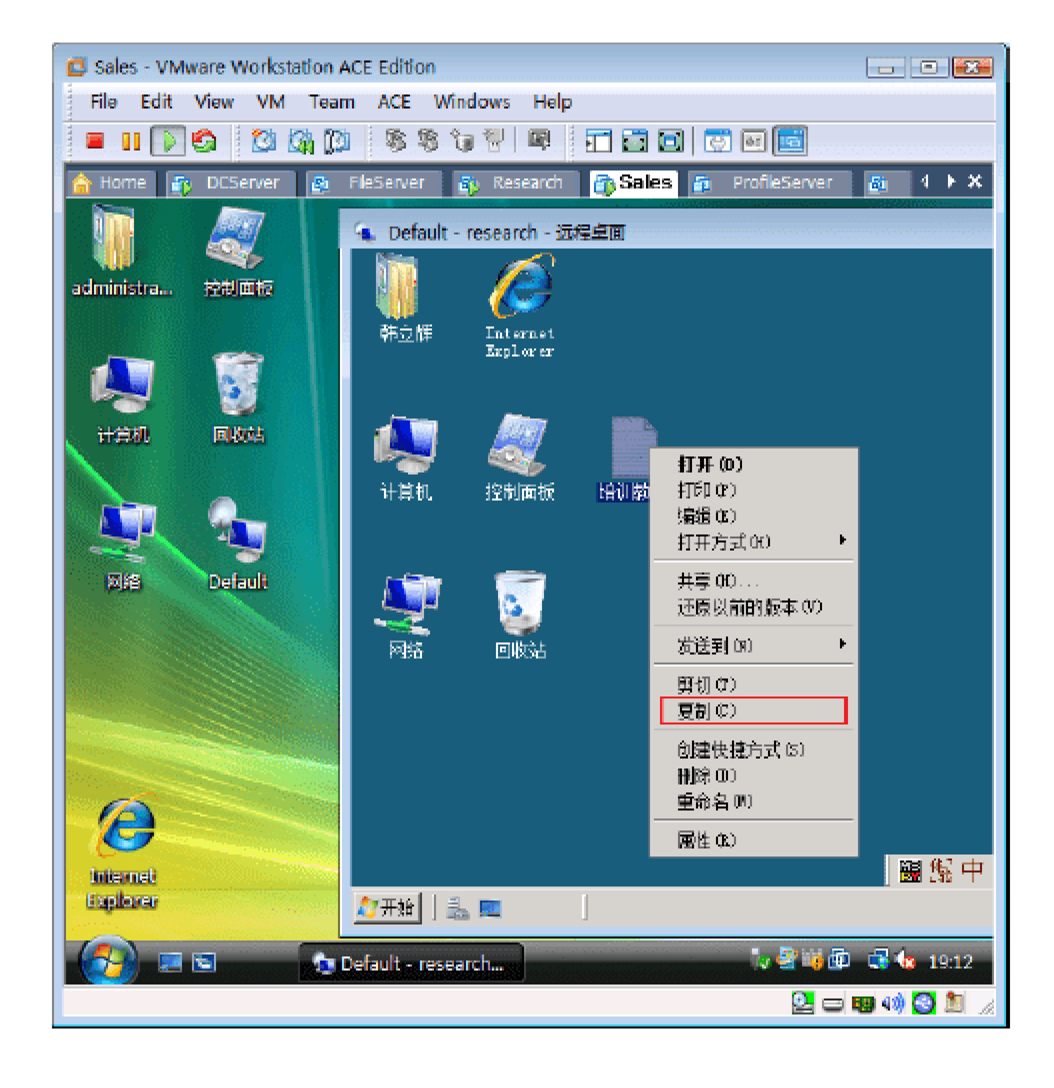




图 12-20　复制远程桌面资源

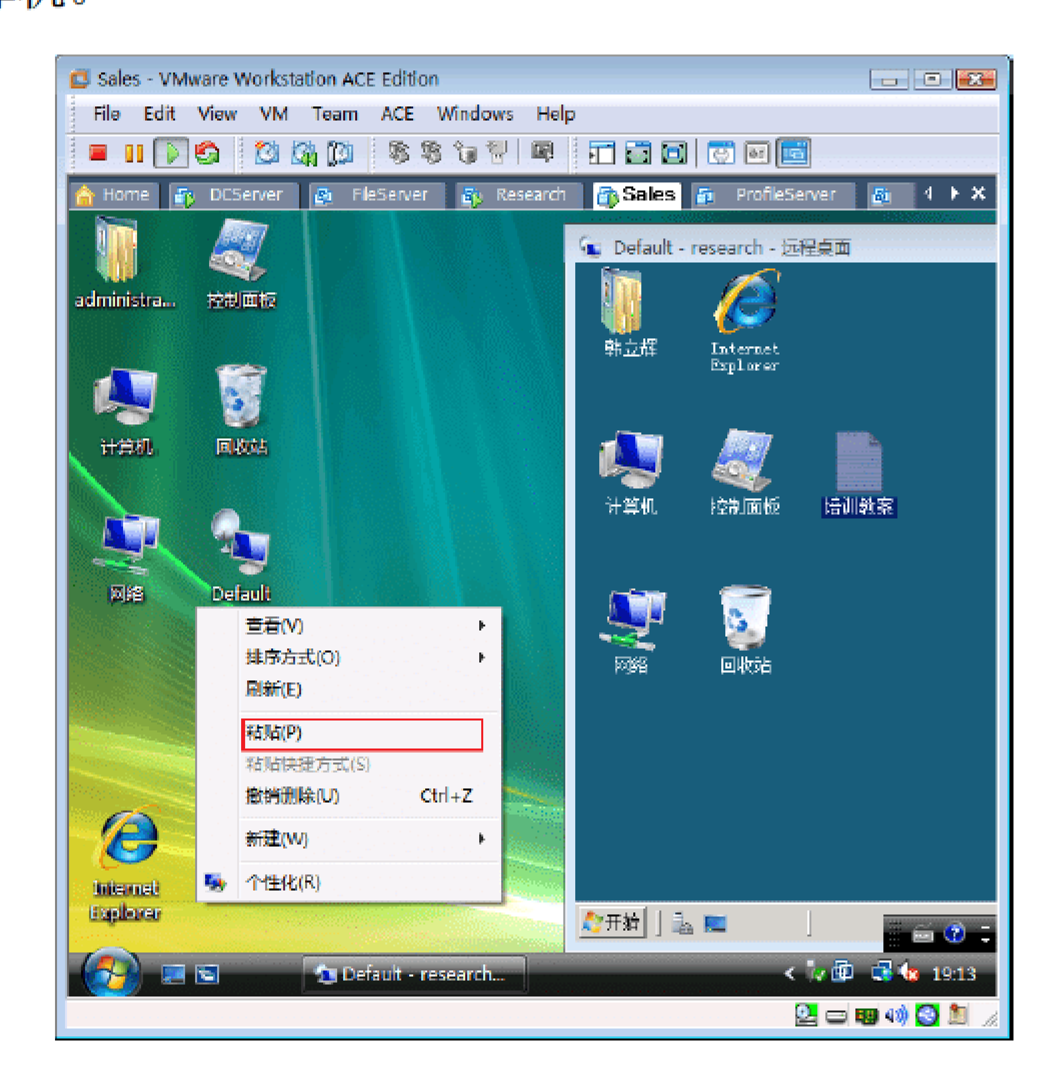


图 12-21　粘贴到本地

12.3.3　配置终端服务单一登录

单一登录是一种身份验证方法，允许具有域账户的用户使用密码或智能卡登录一次，然后，不再要求其提供凭据即可访问远程服务器。

若要在终端服务中实现单一登录功能，应确保满足下列要求。

- 只能对从运行 Windows Vista 的计算机到运行 Windows Server 2008 的终端服务器的远程连接使用单一登录，或者对从一台运行 Windows Server 2008 的服务器到另一台运行 Windows Server 2008 的服务器的远程连接使用单一登录。
- 确保用于登录的用户账户具有相应的权限来登录到终端服务器和 Windows Vista 客户端计算机。
- 客户端计算机和终端服务器必须已加入域。
- 将运行 Windows Vista 的计算机配置为允许使用默认凭据登录到指定的服务器。

使单一登录使用默认凭据

① 以域管理员的账户登录到 Sales。选择“开始”→“运行”命令，在出现的“运行”对话框中输入 gpedit.msc，单击“确定”按钮，打开本地组策略编辑器。

② 在左侧窗格中，展开“计算机配置”→“管理模板”→“系统”节点，然后单击“凭据分配”。

③ 如图 12-22 所示，双击“允许分配默认凭据”。

④ 如图 12-23 所示，在属性对话框的“设置”选项卡中，选中“已启用”单选按钮，然后单击“显示”按钮。

⑤ 在“显示内容”对话框中，单击“添加”按钮，将服务器添加到列表中。

⑥ 在“添加项目”对话框中，在“输入要添加的项目”文本框中，输入前缀 termsrv/，后跟终端服

务器的名称(例如 termsrv/Research)，然后单击“确定”按钮。

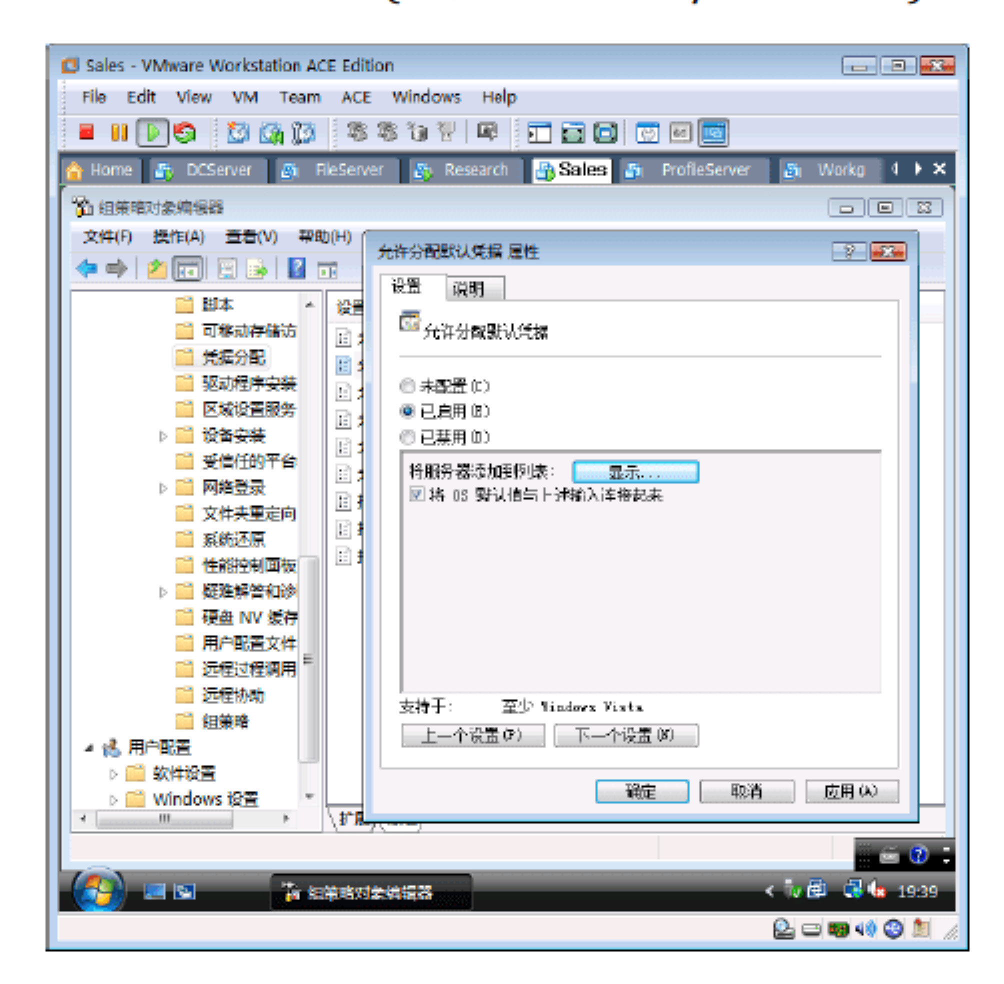


图 12-22　打开凭据分配

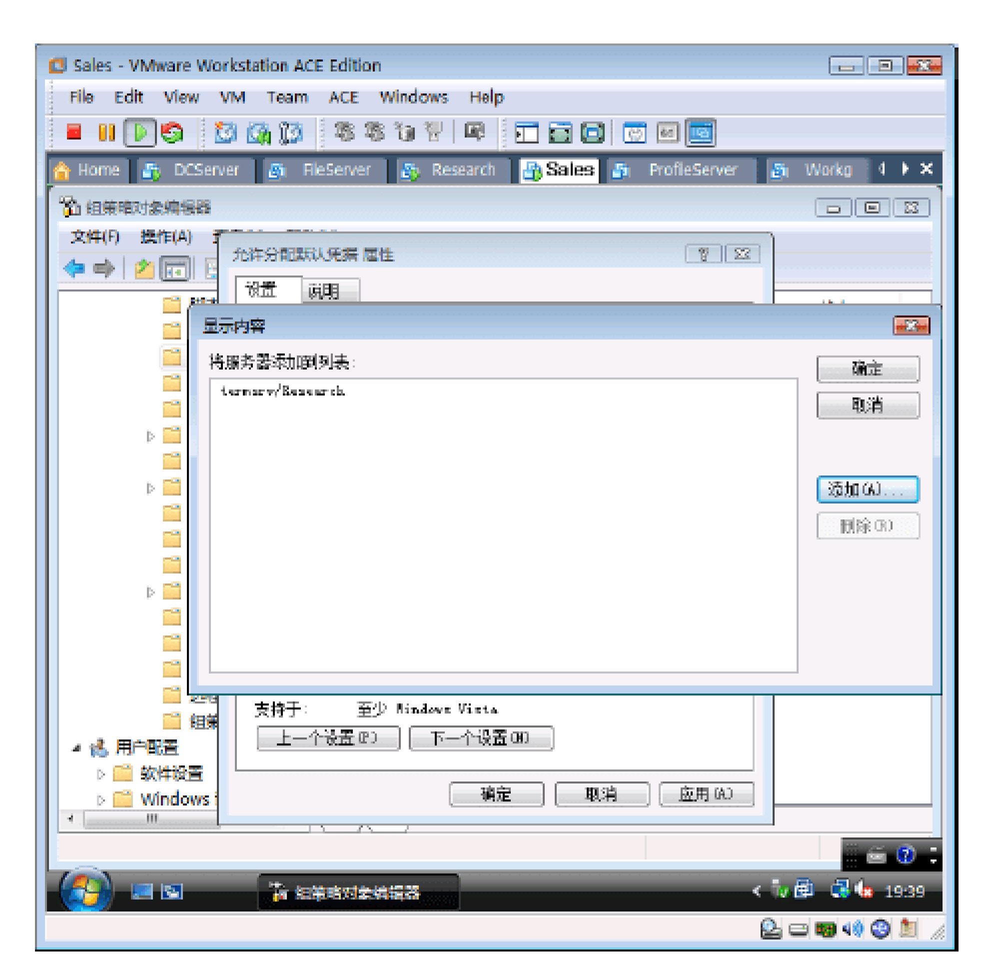


图 12-23　添加项目

⑦　单击“确定”按钮，关闭属性对话框。

⑧　删除存储的网络密码，如图 12-24 所示，以域用户登录到 Sales，再使用远程桌面客户端连接就不需要再次输入密码了。

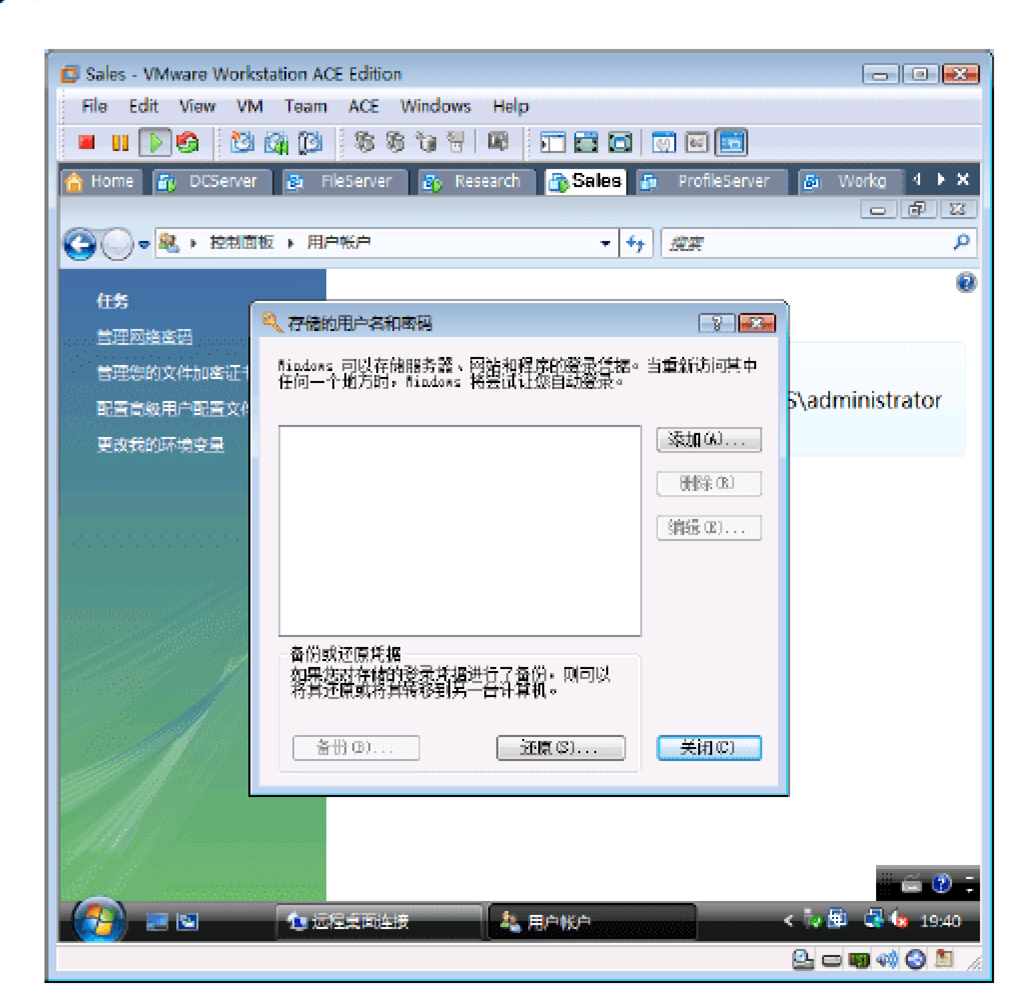


图 12-24　删除存储的网络凭据

12.3.4　配置终端服务连接的安全设置

什么是服务器身份验证选项

在远程桌面连接中，服务器身份验证用于验证用户是否连接到正确的远程计算机或服务器。此安全措施有助于防止连接到非预期的计算机或服务器，以及由此增加的暴露保密信息的可能性。下面有三个可用的身份验证选项，如图 12-25 所示。



图 12-25　服务器身份验证

- “始终连接，即使身份验证失败”(最不安全)：使用此选项，即使远程桌面连接无法验证远程计算机的身份，它仍然会连接。
- “如果身份验证失败则向我发出警告”(较为安全)：使用此选项，如果远程桌面连接无法验证远程计算机的身份，则发出警告，用户可以选择是否继续连接。
- “如果身份验证失败则不连接”(最安全)：使用此选项，如果远程桌面连接无法验证远程计算机的身份，则无法建立连接。

① 在“高级”选项卡中选择“身份验证失败时不连接”选项。如图 12-26 所示，在“显示”选项卡中，选中“全屏显示时显示连接栏”复选框，单击“连接”按钮。

② 如图 12-27 所示，将光标移到顶端，单击 🔒 按钮，可以看到“使用 Kerberos 已验证远程计算机的身份。”的提示。

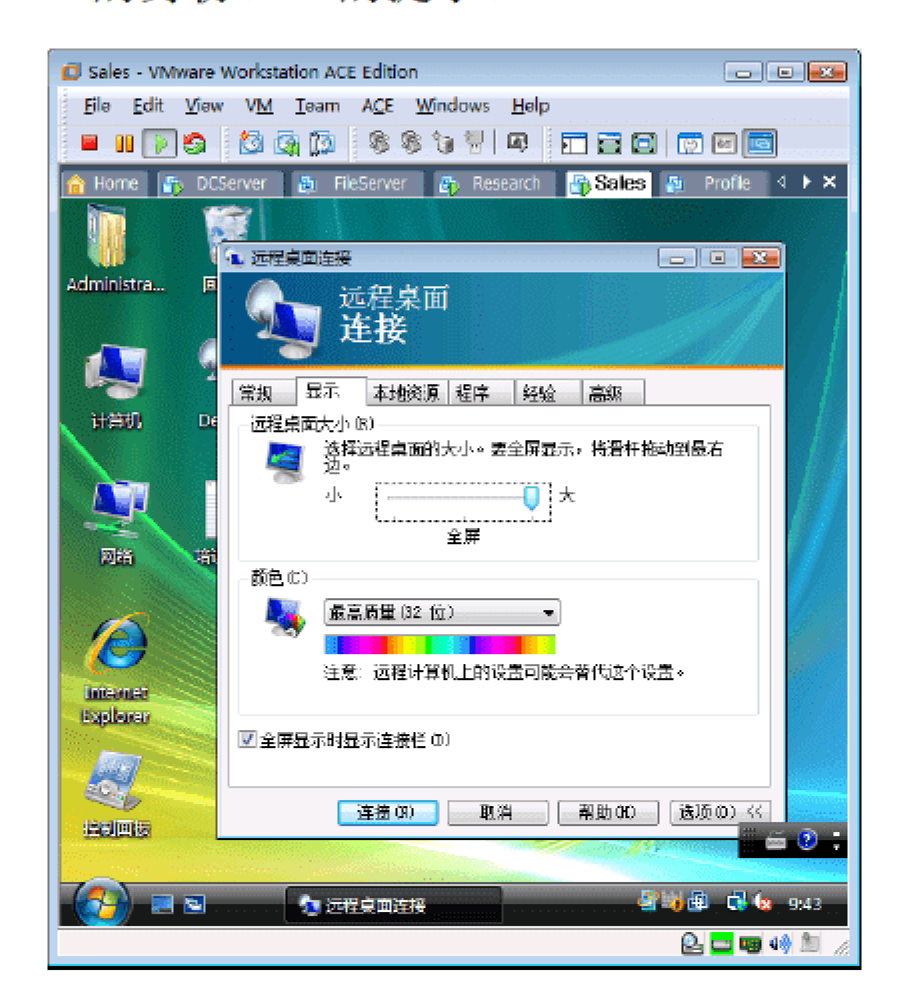


图 12-26　全屏连接

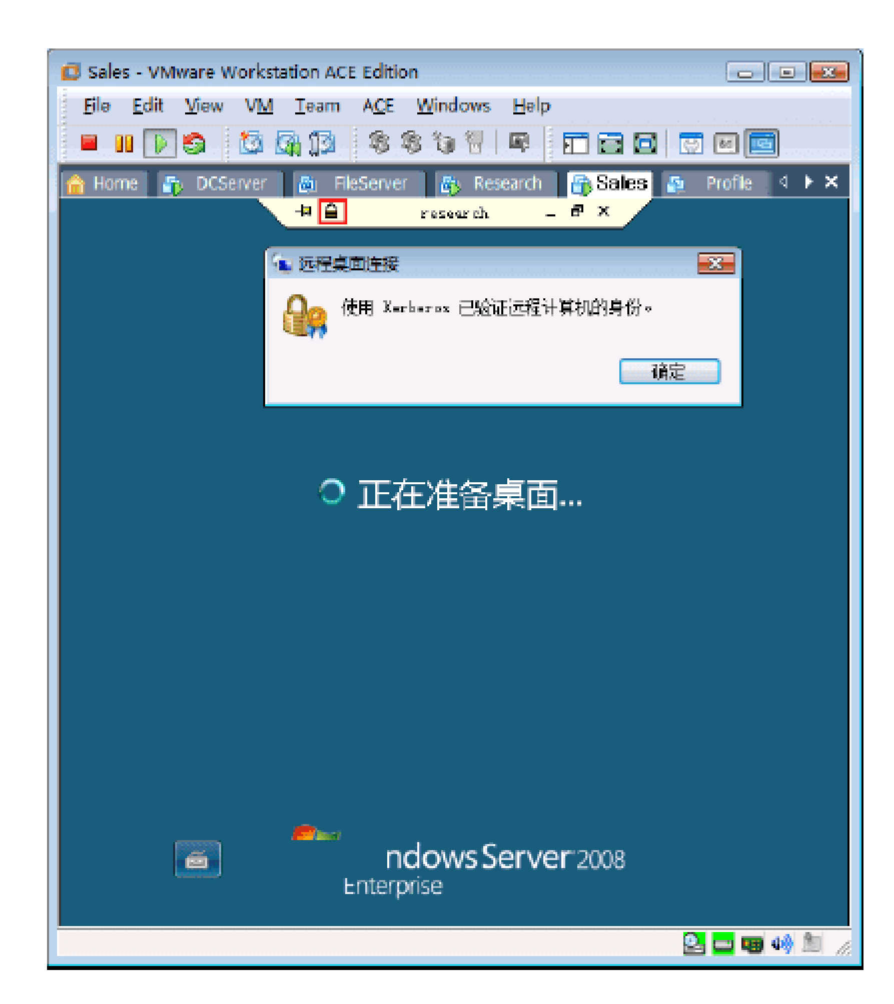


图 12-27　身份验证已经通过

如果不确定选择哪个选项，请向系统管理员或远程计算机的所有者询问。

运行 Windows Server 2003 Service Pack 1 (SP1) 或更早版本操作系统的远程计算机不能提供用于身份验证的身份。如果确认远程计算机运行的是那些早期操作系统之一，则可通过选择“始终连接，即使身

份验证失败”避免发出身份验证警告。



注意：如果希望永久更改服务器身份验证选项，则可将该远程计算机的设置保存到一个 .rdp 文件(该文件包含到特定远程计算机的连接的所有设置)中。若要执行此操作，应在远程桌面连接中选择需要的身份验证级别，然后在“常规”选项卡中单击“保存”或“另存为”按钮。若要在以后连接到同一台远程计算机，双击该 .rdp 文件即可。

12.4　配置终端服务器设置

12.4.1　查看连接到服务器远程桌面的会话

在 Research 服务器上，可以看到哪些用户使用哪些计算机使用远程桌面连接到服务器。

如图 12-28 所示，右击 Research 计算机“开始”菜单空白区域，在弹出的快捷菜单中选择“任务管理器”命令。在“Windows 任务管理器”对话框的“用户”选项卡中，可以看到使用远程桌面连接过来的会话。

在命令行下，输入 netstat –n，可以看到到服务器的远程桌面建立的会话。远程桌面使用的是 TCP 3389 端口。

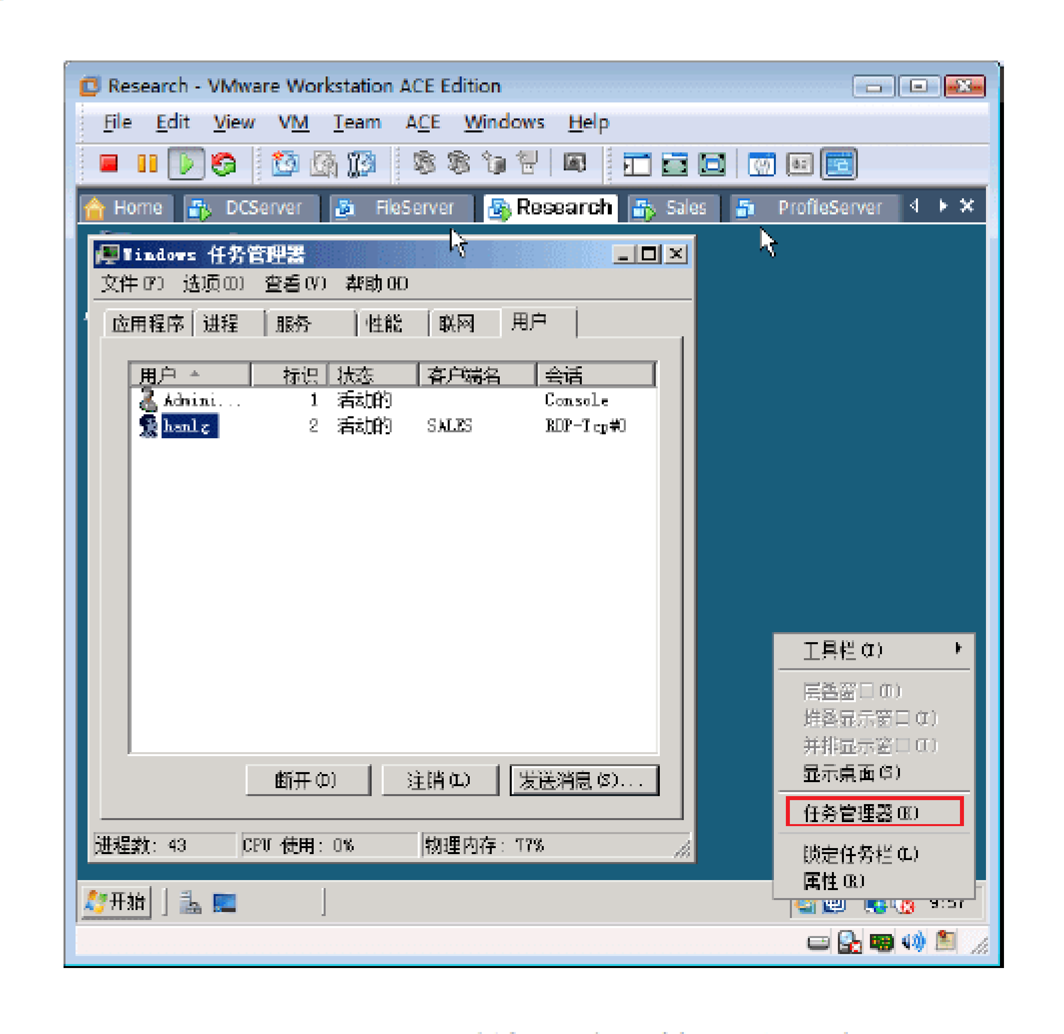


图 12-28　查看使用该计算机的用户

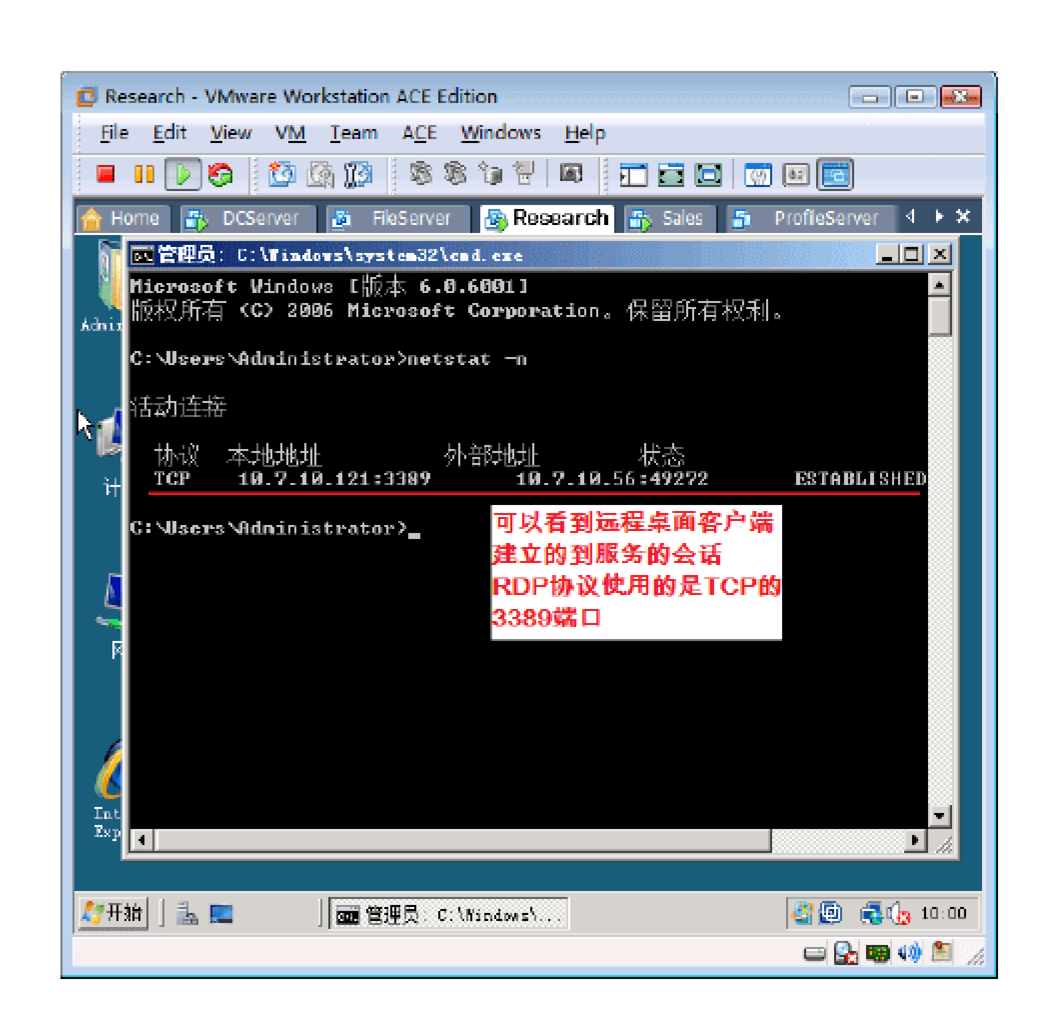


图 12-29　查看终端服务器会话

12.4.2　更改远程桌面使用的默认端口

从安全角度考虑，放到公网上的服务器最好将远程桌面的默认端口改成其他的，这样入侵者就不容易通过端口扫描发现用户服务器开启的远程桌面服务，从而使用户减少受攻击的机会。

以下步骤将会更改服务器的远程桌面的默认端口，并且在高级 Windows 防火墙创建一个 TCP 端口号是 4000 的入站规则。

① 在 Research 计算机中，选择“开始”→“运行”命令，在弹出的“运行”对话框中输入 regedit，单击“确定”按钮。

② 打开注册表编辑工具，依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp 节点。

③ 如图 12-30 所示，单击 PortNumber 选项，在出现的对话框中选中“十进制”单选按钮，可以看到是 3389，改成 4000，单击“确定”按钮。

④ 如图 12-31 所示，重启系统，在命令提示符下输入 netstat –a 查看计算机侦听的端口。可以看到没有 3389，多了一个 4000 端口。

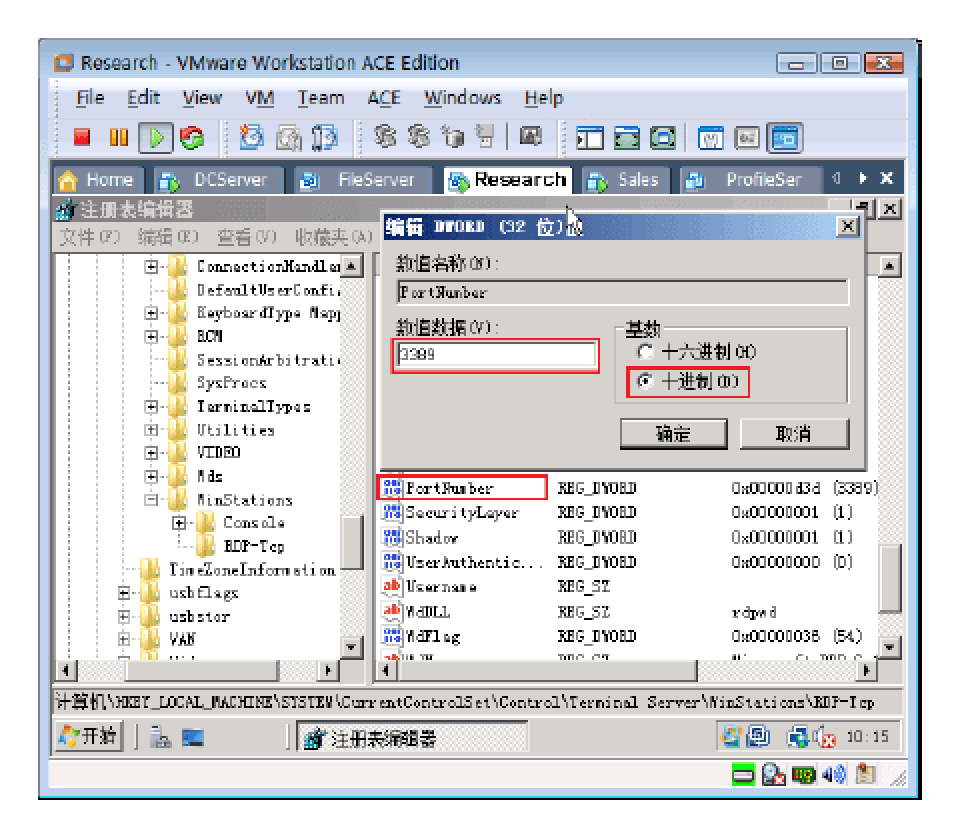




图 12-30　更改注册表

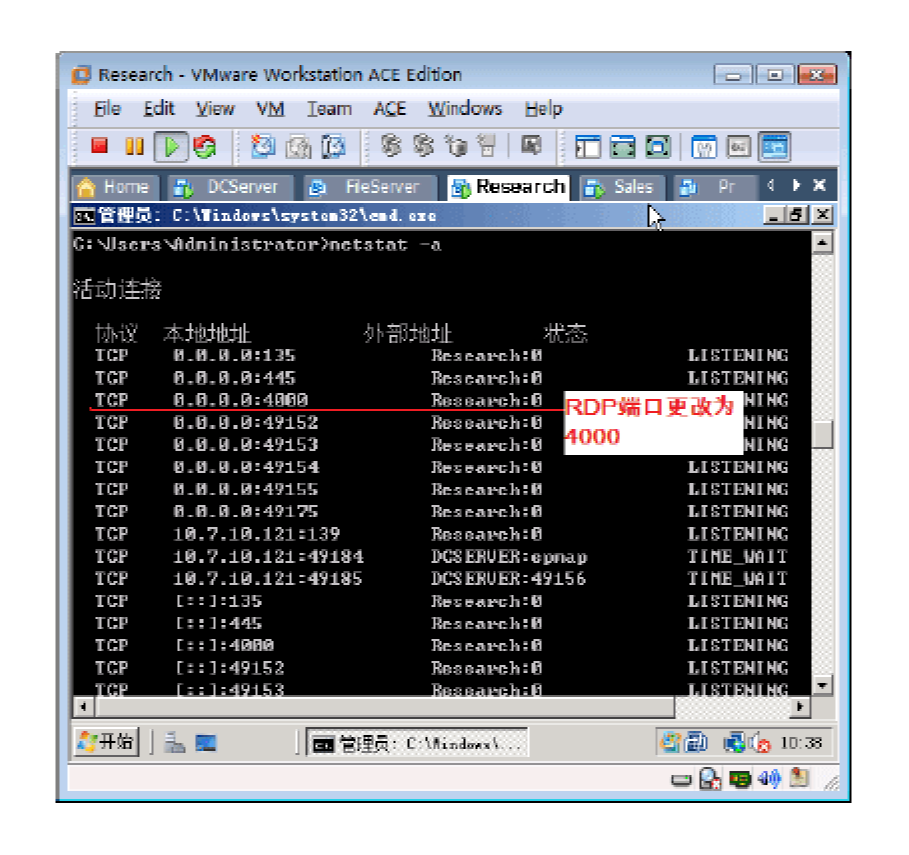


图 12-31　查看侦听的端口

⑤ 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入 wf.msc，打开高级 Windows 防火墙。

⑥ 如图 12-32 所示，当你启用远程桌面，Windows 自动将预置的远程桌面入站规则设置成启用状态。双击该规则可以看到端口是 3389，且不能改。只能创建自己的入站规则了。

⑦ 如图 12-33 所示，右击入站规则，在弹出的快捷菜单中选择“新规则”命令，在出现的对话框中，选中“端口”单选按钮，单击“下一步”按钮。

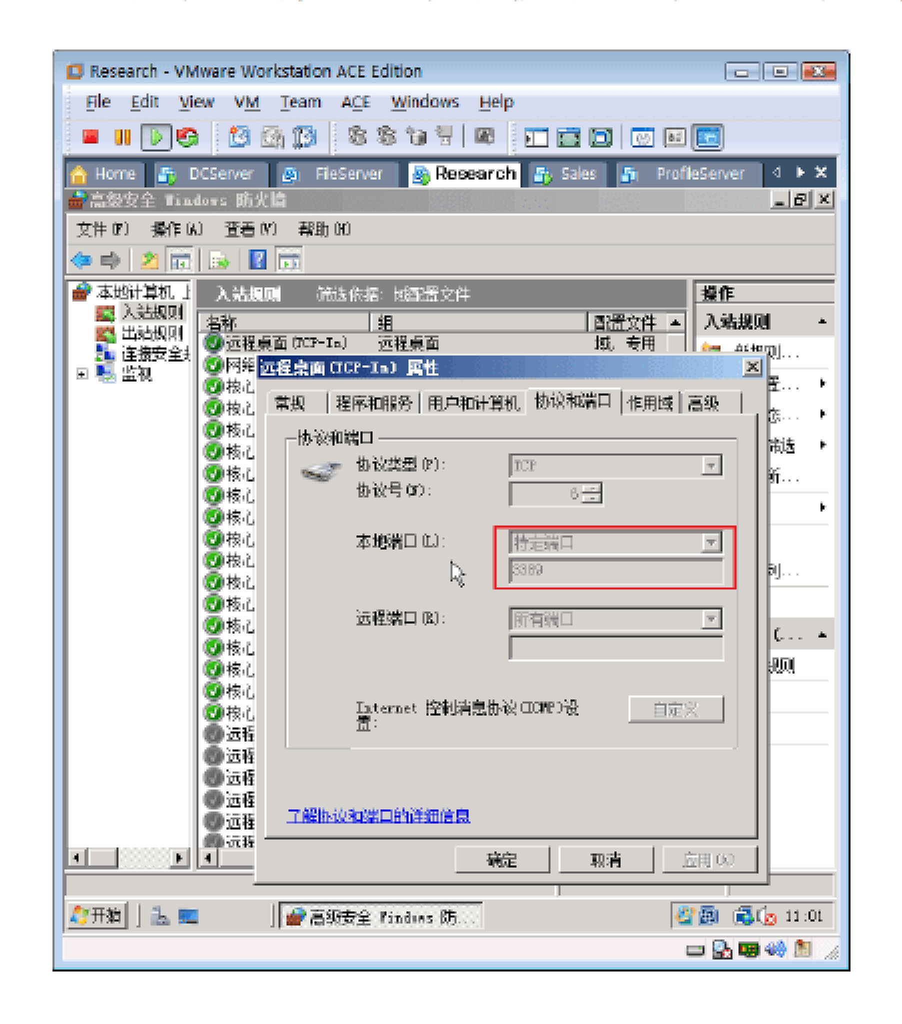


图 12-32　默认允许远程桌面连接的规则

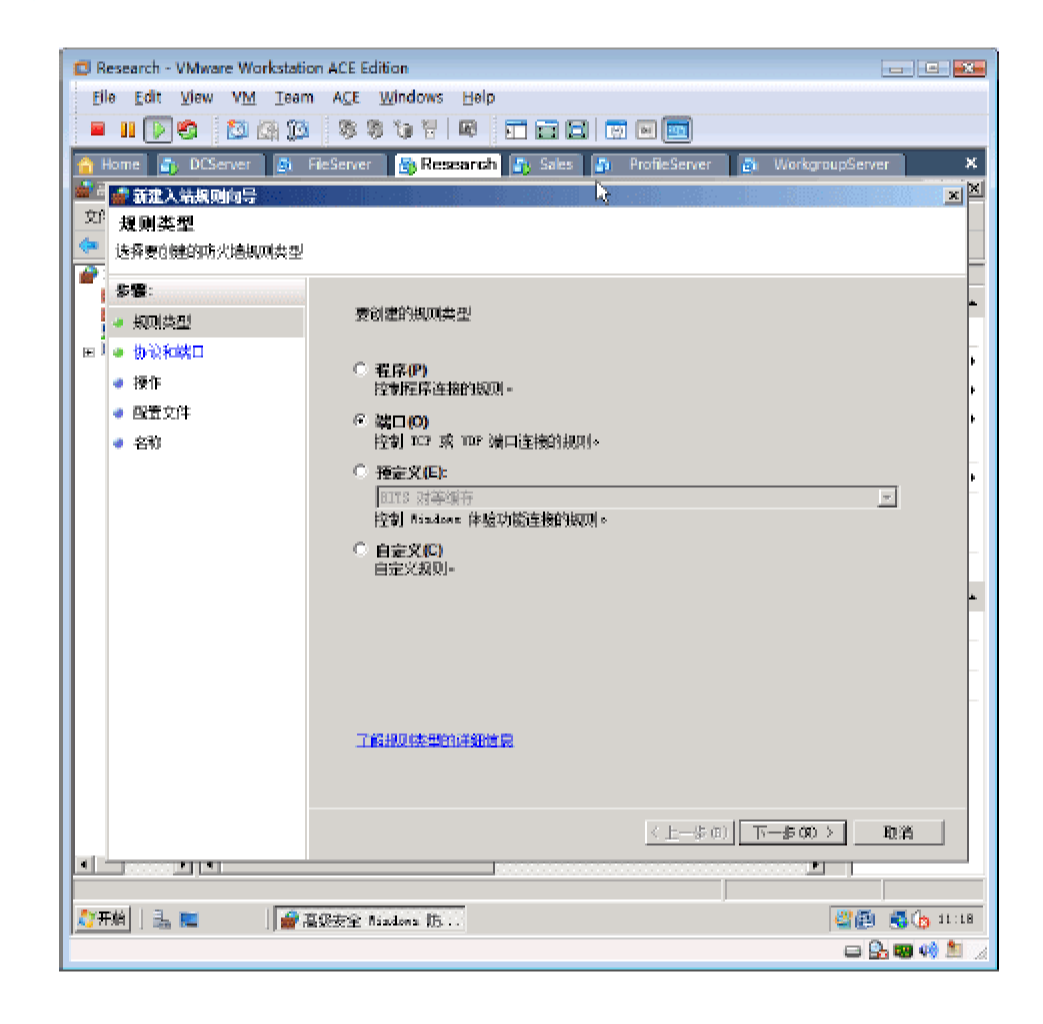


图 12-33　创建新规则

⑧ 如图 12-34 所示，在出现的“协议和端口”界面中，选中 TCP 单选按钮，选中“特定本地端口”单选按钮，输入 4000。单击“下一步”按钮。

⑨ 如图 12-35 所示，在出现的“操作”界面中，选中“允许连接”单选按钮，单击“下一步”按钮。

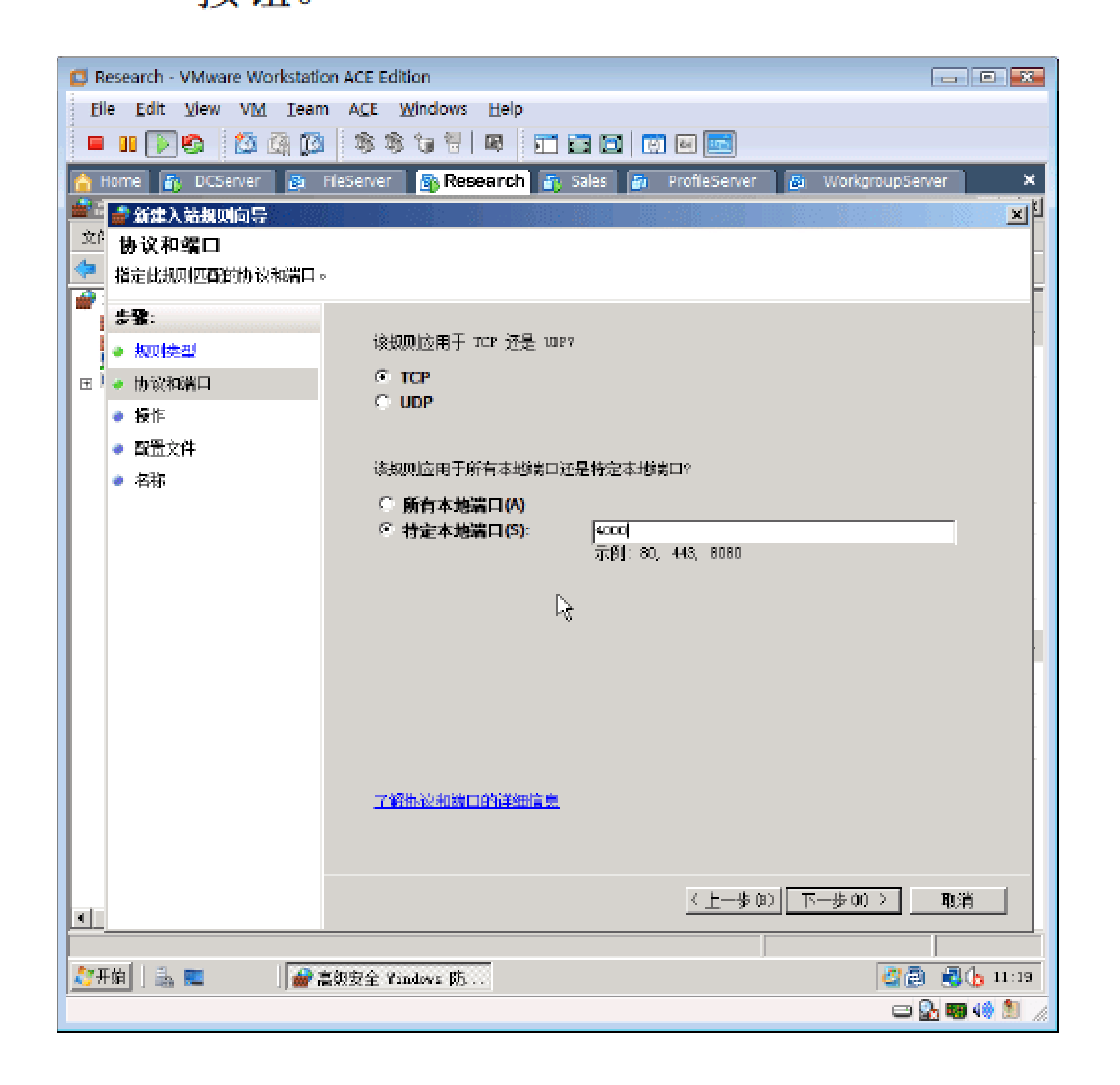


图 12-34 选择协议和端口

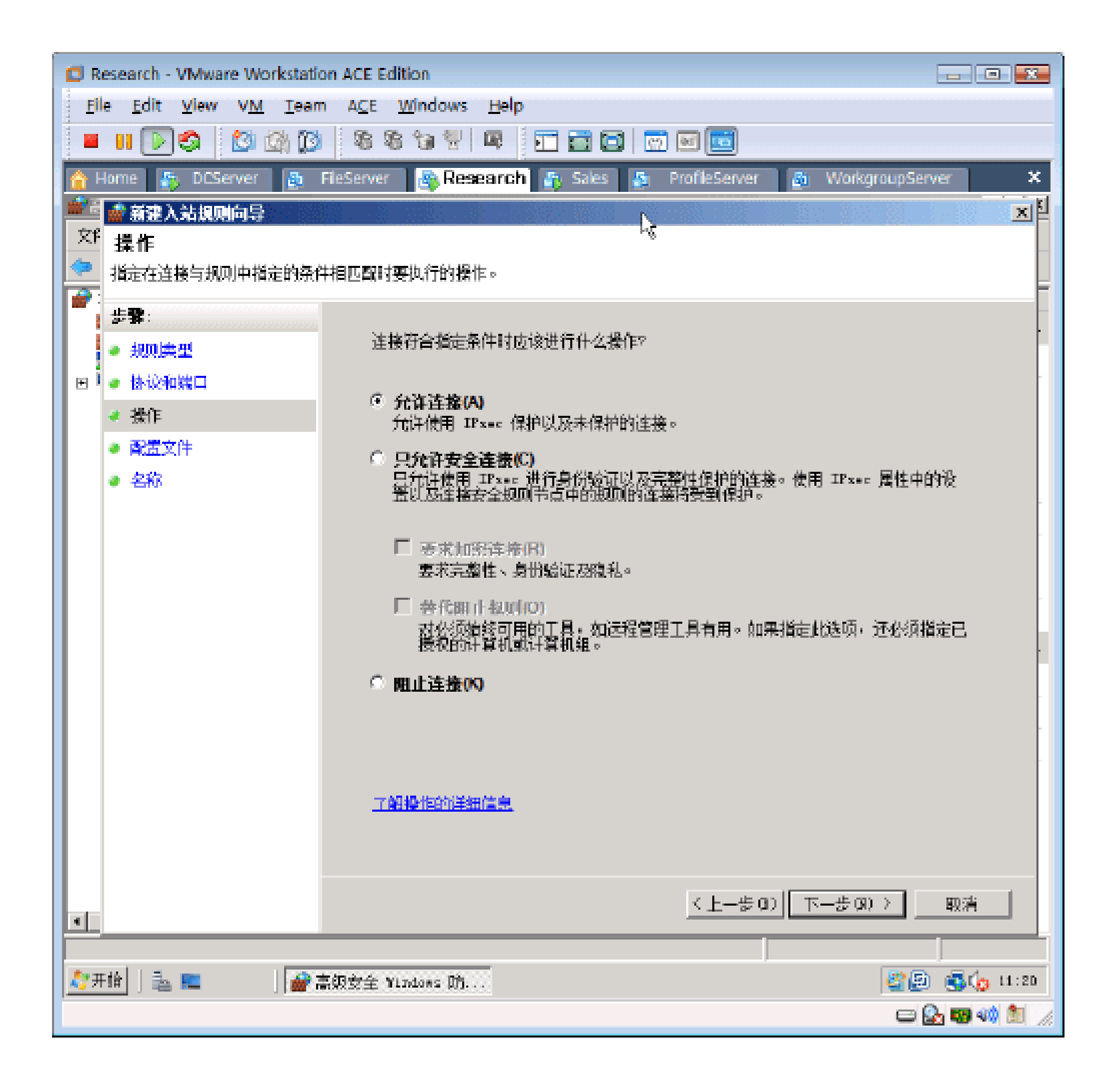


图 12-35 选择操作

⑩ 如图 12-36 所示，在出现的“配置文件”界面中，单击“下一步”按钮。

⑪ 如图 12-37 所示，在出现的“名称”界面中，输入 RDP 4000，单击“完成”按钮。

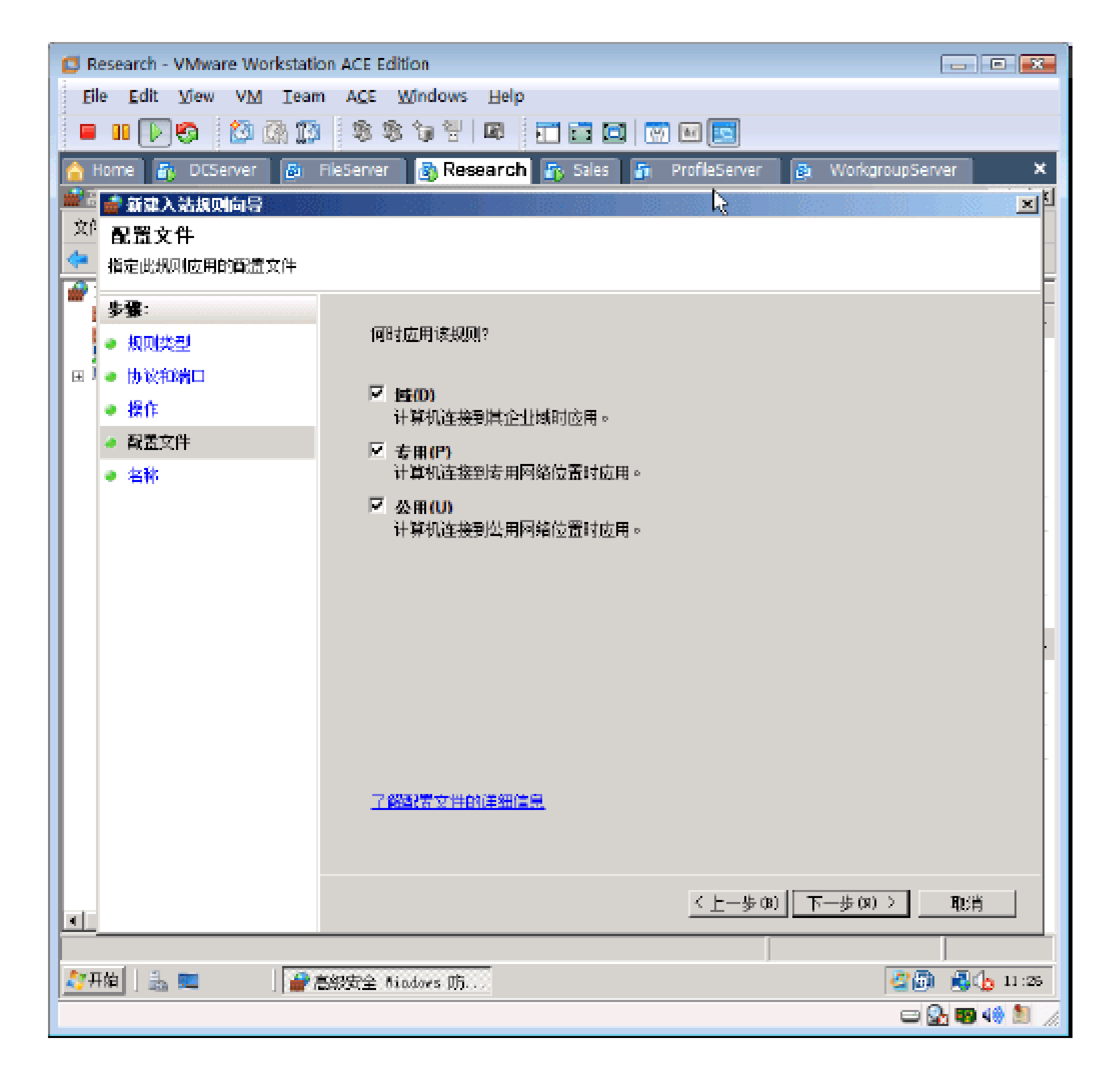


图 12-36 选择配置文件

图 12-37 指定规则名称

⑫ 如图 12-38 所示，在 Vista 上使用 4000 端口连接 Research 的远程桌面。在远程桌面客户端输入 research:4000，单击“连接”按钮。

⑬ 如图 12-39 所示，可以看到连接时，用的是 4000 端口。

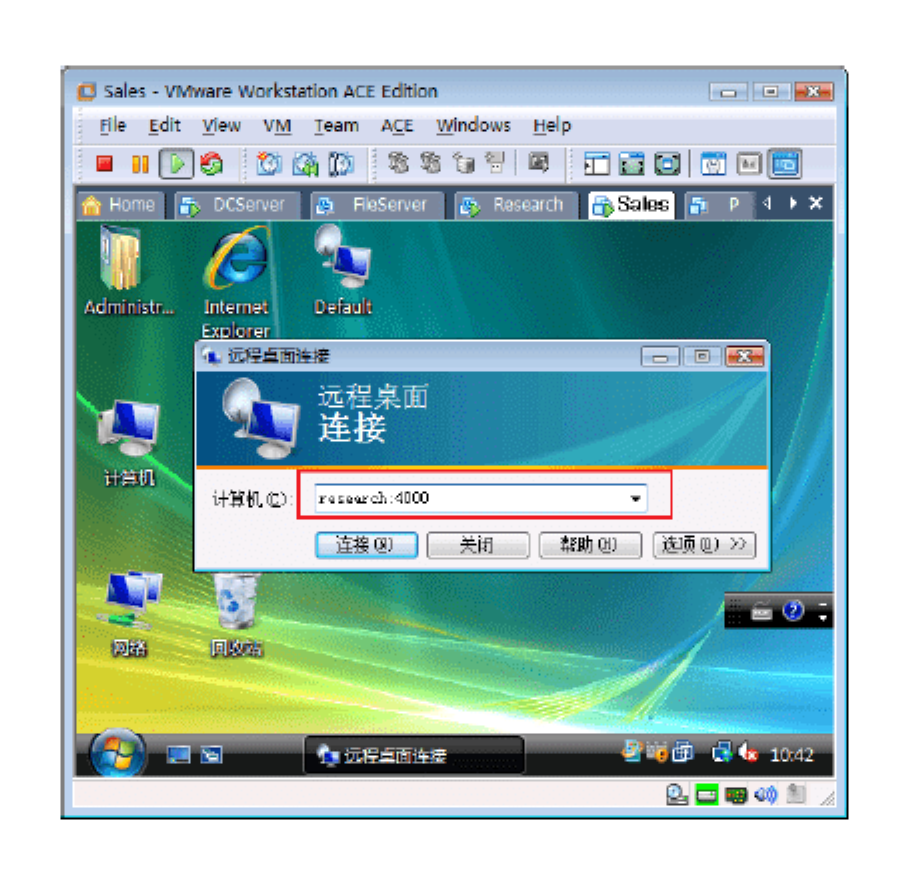


图 12-38　设置 4000 端口连接

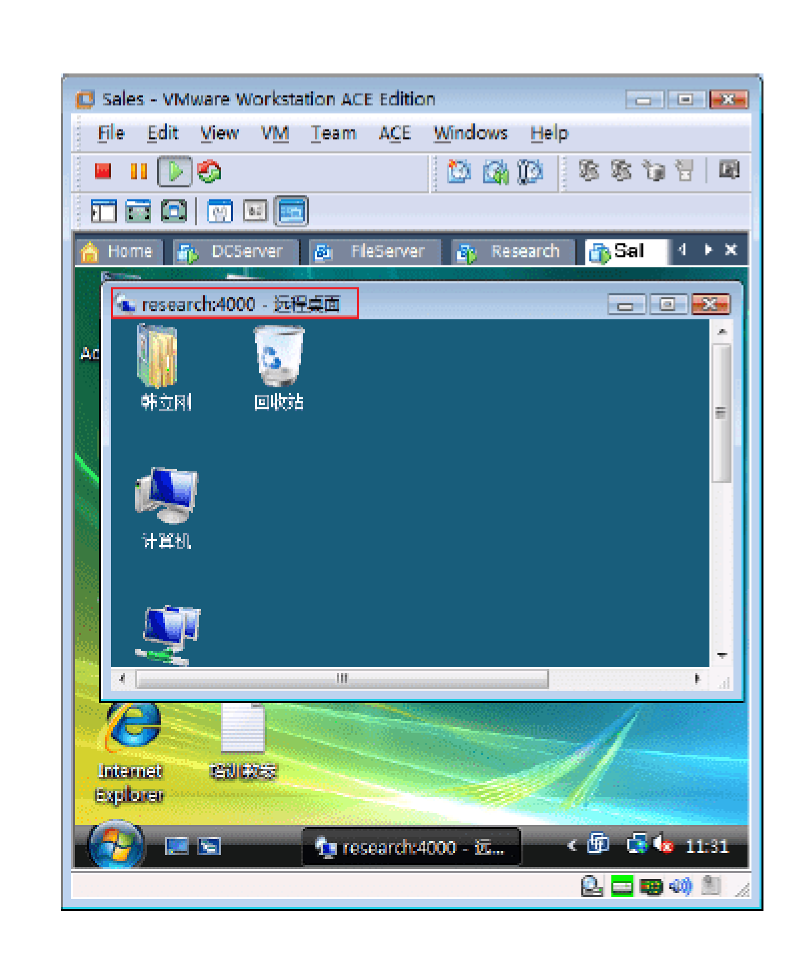


图 12-39　使用 4000 端口连接

12.4.3　限制用户只能进行一个会话

为了提高终端服务器的性能，可以限制用户只能进行一个会话(活动或已断开)。通过限制用户在终端服务器上只能进行一个会话，可以最大限度地减少在终端服务器上创建的远程会话数。这样有助于节省终端服务器上的系统资源，因此，使更多的用户可以连接到终端服务器。

如果将终端服务器配置为限制用户只能进行一个会话，并且用户将该会话置于断开状态，用户下次连接到终端服务器时，将自动重新连接到该会话。

默认情况下，将终端服务器配置为限制用户只能进行一个会话。

① 选择“开始”→“程序”→“管理工具”命令，打开“终端服务配置”窗口。

② 在“常规”选项区中，双击“限制每个用户只能进行一个会话”选项。

③ 如图 12-40 所示，在“属性”对话框的“常规”选项卡中，选择最适合用户环境的“限制每个用户只能进行一个会话”的设置，然后单击“确定”按钮。

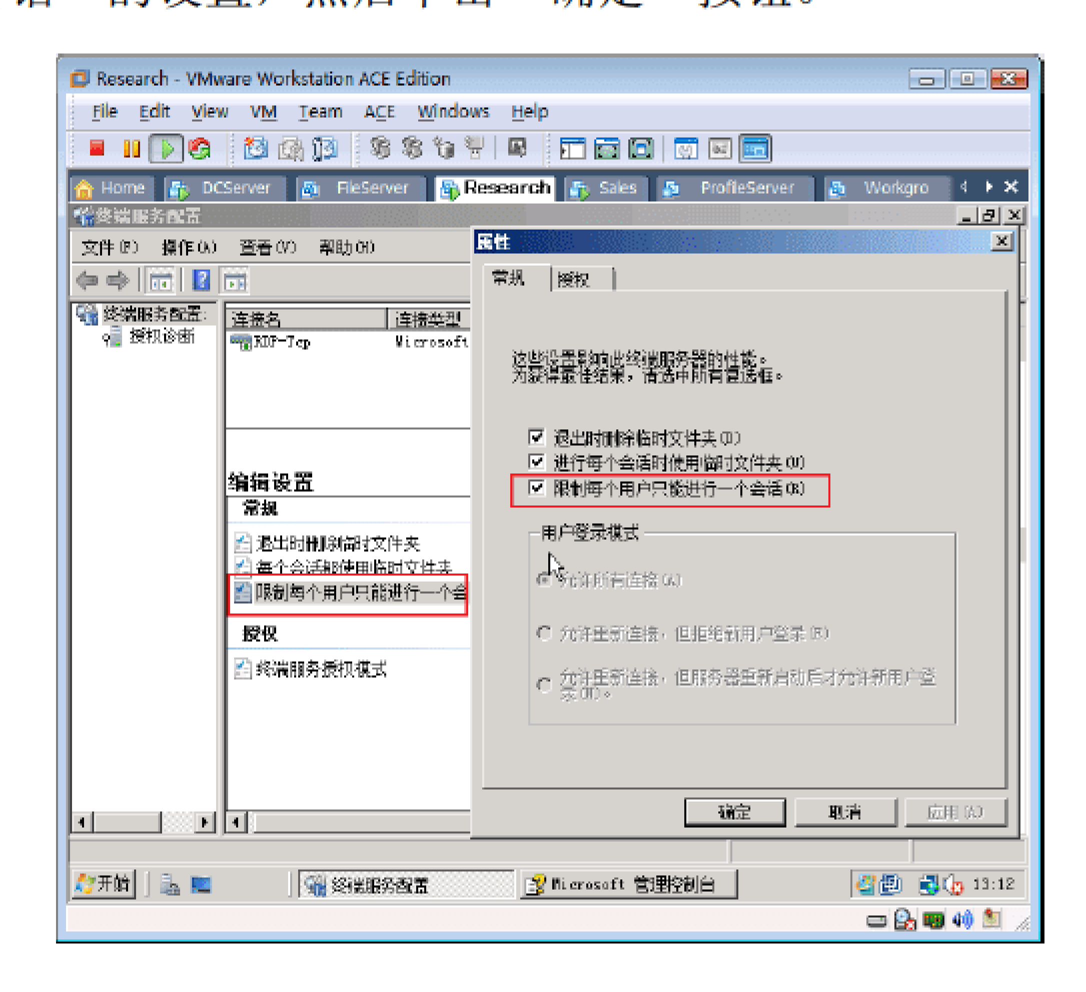


图 12-40　限制每个用户只能进行一个会话

注意：限制每个用户只能进行一个会话时，如果在 Sales 计算机上连接 Research 计算机的远程桌面账号和在控制台登录的账号是同一个账号，会自动将控制台登录的用户注销，如图 12-41 所示。如果控制台用户登录会将 Sales 上的远程桌面断开。

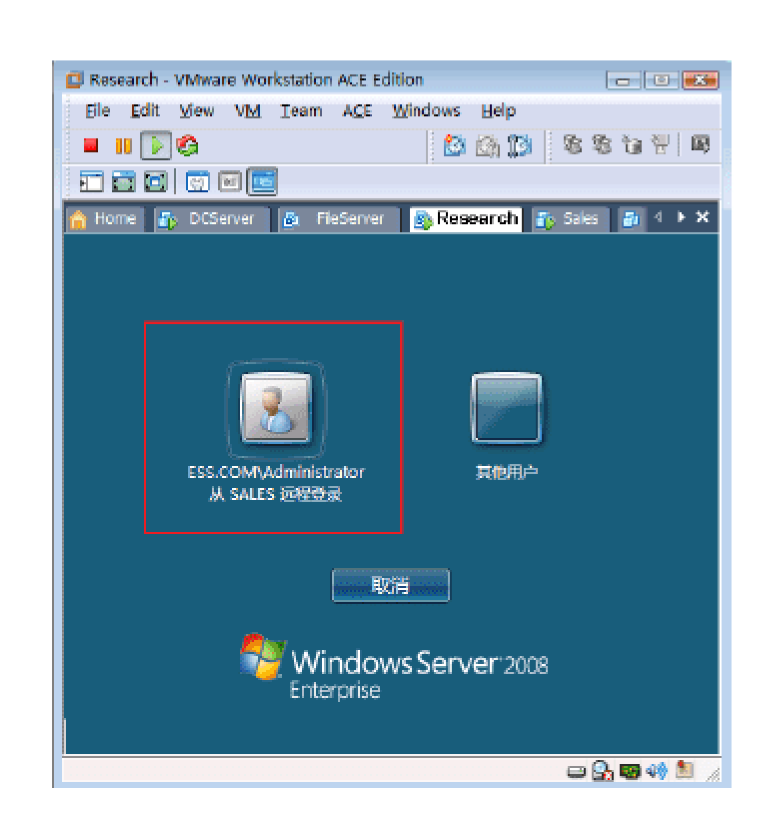


图 12-41　注销当前用户

12.4.4　配置服务器身份验证和加密级别

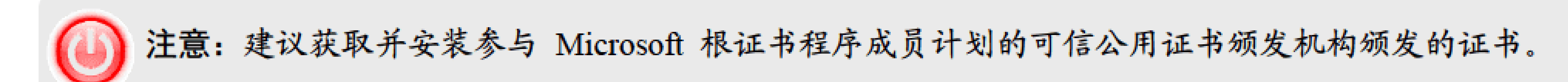
默认情况下，终端服务会话使用本机远程桌面协议（RDP）加密。但是，RDP 不提供身份验证来验证终端服务器的身份。使用传输层安全性 TLS 1.0 进行服务器身份验证并对终端服务器通信进行加密，可以提高终端服务会话的安全性。只有正确地配置了终端服务器和客户端计算机，TLS 才能提高安全性。

可以使用三个安全层。

- SSL (TLS 1.0)：将用于服务器身份验证以及对服务器与客户端之间传输的所有数据进行加密。
- 协商：这是默认设置，将使用客户端支持的最安全的安全层。如果支持 SSL (TLS 1.0)，则使用 SSL (TLS 1.0)。如果客户端不支持 SSL (TLS 1.0)，则使用 RDP 安全层。
- RDP 安全层：服务器与客户端之间的通信将使用本机 RDP 加密。如果选择 RDP 安全层，则无法使用网络级身份验证。

注意：在客户端连接到终端服务器时，可以通过在连接过程的早期提供用户身份验证来提高终端服务器的安全性。这种早期用户身份验证方法称为网络级身份验证。有关网络级身份验证的详细信息，请参阅为终端服务连接配置网络级身份验证。

使用 SSL (TLS 1.0) 在 RDP 连接期间保护客户端与终端服务器之间的通信时，需要使用证书对终端服务器进行身份验证。可以选择已安装在终端服务器上的证书，也可以使用默认的自签名证书。


注意：建议获取并安装参与 Microsoft 根证书程序成员计划的可信公用证书颁发机构颁发的证书。

对于终端服务连接，数据加密可以通过在客户端与服务器之间的通信链路上进行加密来保护用户的数据。加密有助于抵御在服务器与客户端之间的链路上未经授权截获传输数据的风险。

默认情况下，以可用的最高安全级别对终端服务连接进行加密。但是，某些旧版本的终端服务客户端

不支持此高级别的加密。如果网络中包含此类旧版客户端，可以将连接的加密级别设置为以客户端支持的最高加密级别发送和接收数据。

注意： 若要确定计算机上运行的远程桌面连接版本支持的最大加密强度，请启动“远程桌面连接”，单击“远程桌面连接”对话框左上角的图标，然后单击“关于”按钮。在“关于远程桌面连接”对话框中查找“最大加密强度”。Remote Desktop Connection 5.2 以及更高版本支持 128 位的加密。

可以使用以下四个加密级别。

- 符合 FIPS 标准。此级别使用经过联邦信息处理标准 (FIPS) 140-1 验证的加密方法，对从客户端向服务器发送的数据以及从服务器向客户端发送的数据进行加密和解密。不支持此加密级别的客户端无法连接。
- 高。此级别使用 128 位加密对从客户端向服务器发送的数据以及从服务器向客户端发送的数据进行加密。终端服务器在只包含 128 位客户端(例如远程桌面连接客户端)的环境中运行时使用此级别。不支持此加密级别的客户端无法连接。
- 客户端兼容。这是默认设置，此级别以客户端支持的最大密钥强度对在客户端与服务器之间发送的数据进行加密。终端服务器在包含混合客户端或旧版客户端的环境中运行时使用此级别。
- 低。此级别使用 56 位加密对从客户端向服务器发送的数据进行加密。不对从服务器向客户端发送的数据进行加密。

操作步骤如下。

① 选择“开始”→“管理工具”→“终端服务”命令，然后单击“终端服务配置”选项。

② 在“连接”选项组中，右击相应的连接名，然后从弹出的快捷菜单中选择“属性”命令。

③ 在该连接的属性对话框中，切换到“常规”选项卡，如图 12-42 所示。

根据你的安全要求以及客户端计算机可以支持的安全级别，选择适合你的环境的服务器身份验证设置和加密设置。

如果选择 SSL (TLS 1.0)，则选择终端服务器上安装的某个证书，或单击“默认”按钮生成自签名证书。如果使用的是自签名证书，证书名称将显示为“已自动生成”。

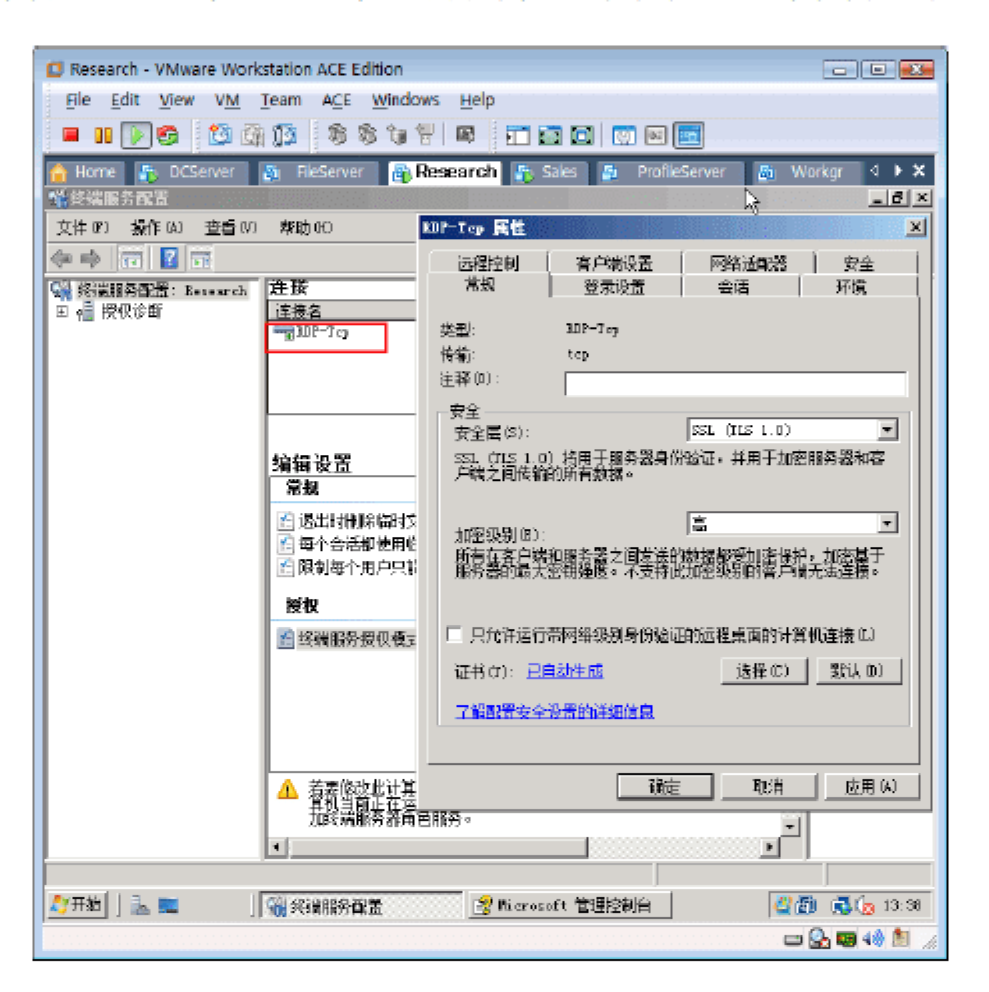


图 12-42 配置安全级别

④　单击“确定”按钮。

12.4.5　为终端服务连接配置网络级身份验证

在客户端连接到终端服务器时，可以通过在连接过程的早期提供用户身份验证来提高终端服务器的安全性。这种早期用户身份验证方法称为网络级身份验证。

网络级身份验证是一种新的身份验证方法，在用户建立远程桌面连接并出现登录屏幕之前完成用户身份验证。这是比较安全的身份验证方法，有助于保护远程计算机避免恶意用户和恶意软件的攻击。网络级身份验证的好处如下。

- 最初需要较少的远程计算机资源。验证用户之前，远程计算机使用有限的资源，而不是像以前版本那样启动完整的远程桌面连接。
- 可以通过降低受到拒绝服务攻击的风险，帮助提高安全性。

若要使用网络级身份验证，需要满足下列所有要求。

- 在客户端计算机上，需要至少使用 Remote Desktop Connection 6.0。
- 在客户端计算机上，需要使用支持凭据安全的程序（CredSSP）协议的操作系统(例如 Windows Vista)。
- 在终端服务器上，需要使用 Windows Server 2008。

为终端服务连接配置网络级身份验证的操作如下。

①　选择“开始”→“管理工具”→“终端服务”命令，然后单击“终端服务配置”选项。

②　在“连接”选项区中，右击相应的连接名，然后从弹出的快捷菜单中选择“属性”命令。

③　在该连接的属性对话框中，切换到“常规”选项卡。

④　如图 12-43 所示，选中“只允许运行带网络级别身份验证的远程桌面的计算机连接”复选框。

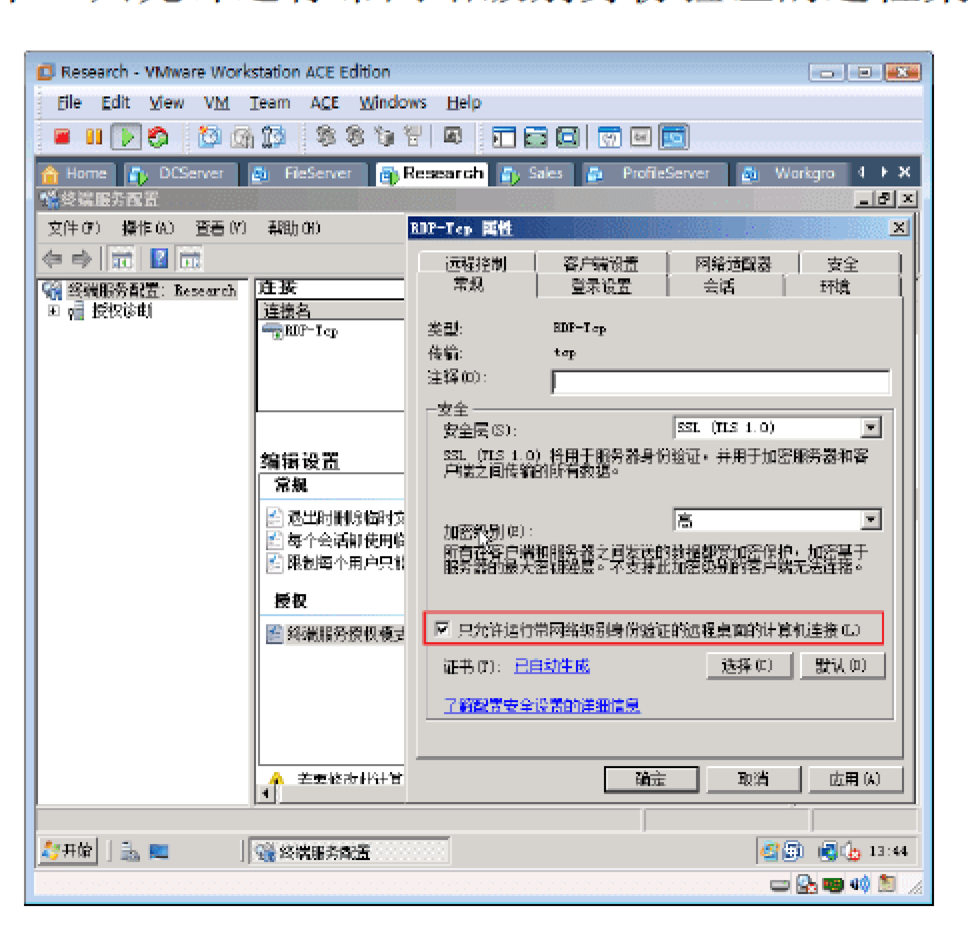


图 12-43　网络级身份验证

> **提示**：如果“只允许运行带网络级别身份验证的远程桌面的计算机连接”复选框已选中并灰显，则已启用“要求使用网络级别身份验证对远程连接进行用户身份验证”组策略设置并应用于终端服务器。

⑤　单击“确定”按钮。

12.4.6 配置终端服务连接的权限

若要远程连接到终端服务器，用户必须提供凭据，以便进行身份验证，并使终端服务器可以确定用户有权执行的操作。

默认情况下，连接将使用用户提供的登录信息，用户使用远程桌面连接远程连接到终端服务器时提供这些信息。

如果不使用客户端提供的登录信息，可以在连接的属性对话框的“登录设置”选项卡中指定用于该连接的登录信息。

还可以指定在连接到终端服务器时，始终提示用户提供密码，即使用户已将远程桌面连接配置为使用已保存的凭据连接到终端服务器时也是如此。

配置连接的登录设置

① 选择“开始”→“程序”→“管理工具”→“终端服务”命令，然后单击“终端服务配置”选项。

② 在“连接”选项区中，右击相应的连接名，然后从弹出的快捷菜单中选择“属性”命令。

③ 在该连接的属性对话框中，切换到“登录设置”选项卡。

④ 如图 12-44 所示，选中“始终提示密码”单选按钮，单击“确定”按钮。

如图 12-45 所示，如果服务器对内网开放或用户在网络层实现了安全设置，可以选中“始终使用以下登录信息”单选按钮，这样用户使用远程桌面登录时不需要输入账号和密码，总是以用户指定的用户身份登录。

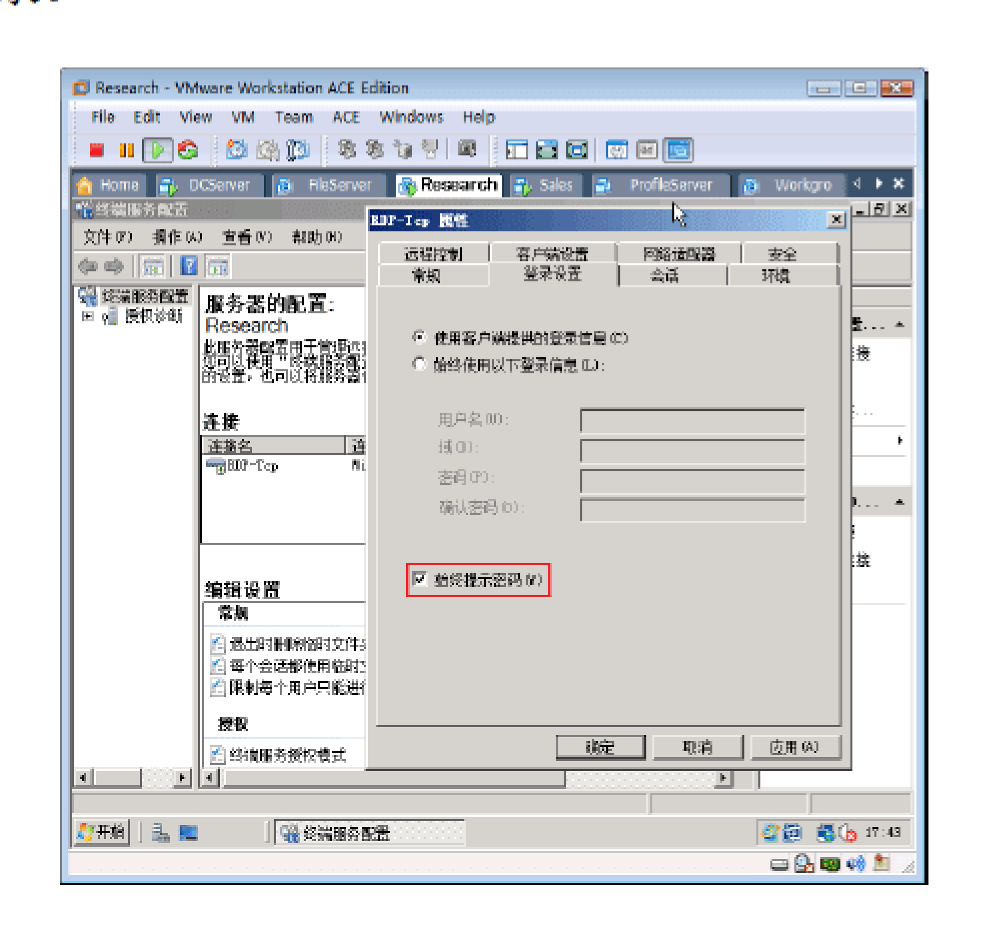


图 12-44 始终提示密码

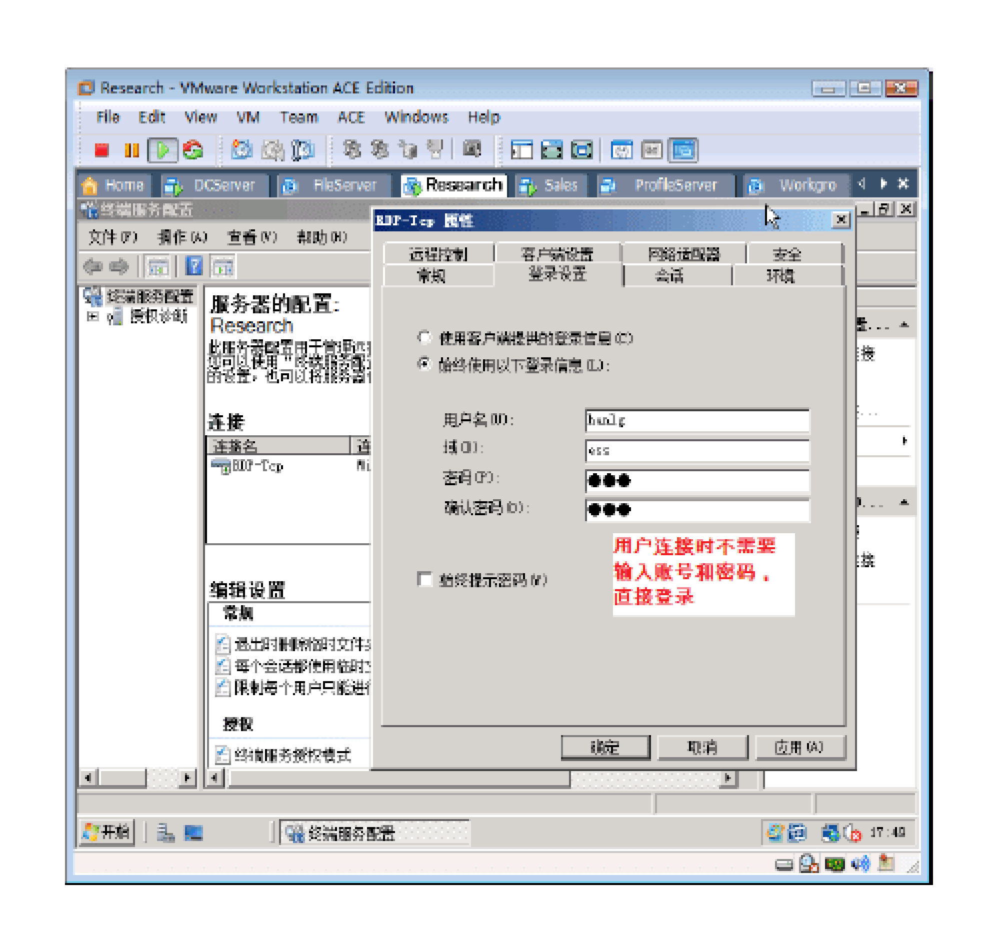


图 12-45 始终使用指定账户连接

12.4.7 使本地设备和资源可以在远程会话中访问

通过终端服务，用户可以在远程会话中访问其本地设备和资源。用户可以访问本地驱动器、打印机、剪贴板和受支持的即插即用设备等资源。这通常称为重定向。

在 Windows Server 2008 中，重定向已得到增强和扩展。现在可以重定向 Windows 便携设备，尤其是基于媒体传输协议（MTP）的媒体播放机和基于图片传输协议（PTP）的数码相机。

在 Windows Server 2008 中，还可以重定向使用 Microsoft Point of Service (POS) for .NET 1.1 的设备。只有终端服务器运行的是基于 x86 版本的 Windows Server 2008 时，才支持重定向 Microsoft POS for .NET 设备。

如图 12-46 所示，用户可以在远程桌面连接的“客户端设置”选项卡中指定要重定向到远程计算机的设备和资源的类型。

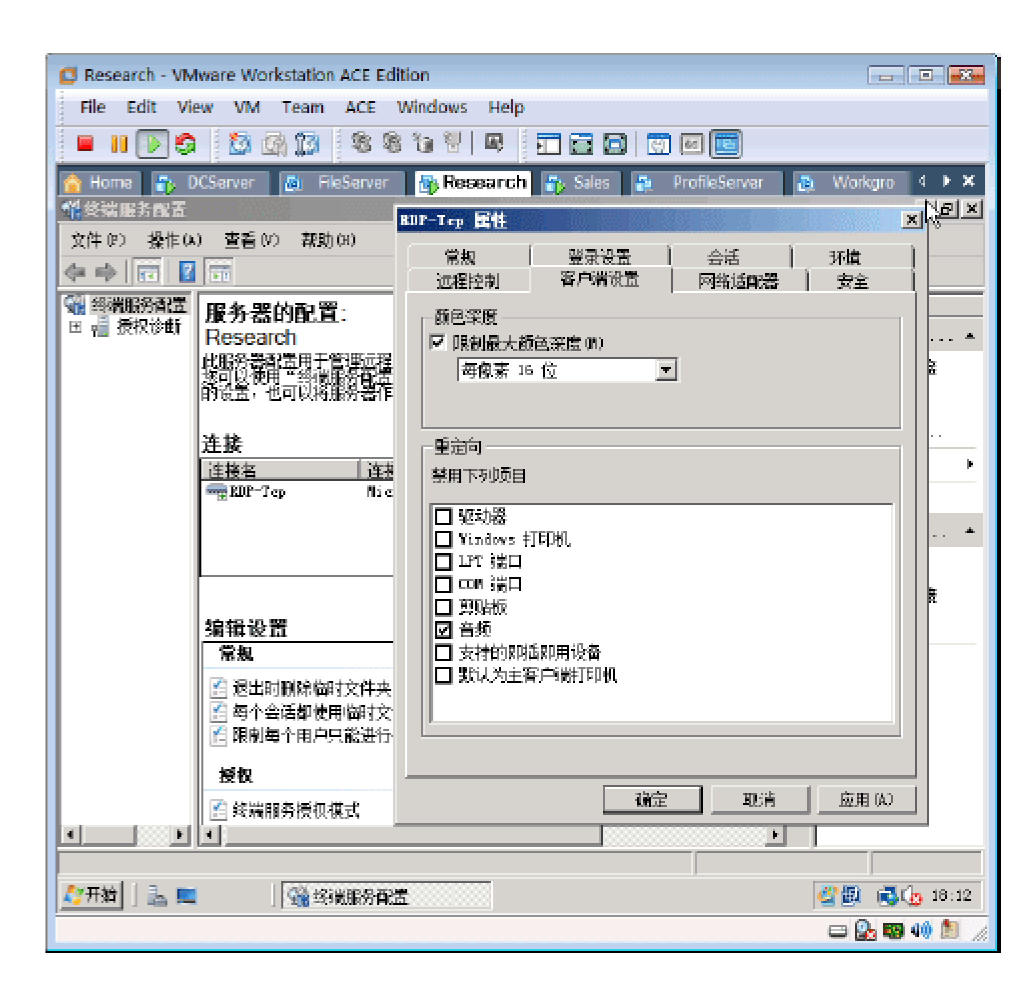
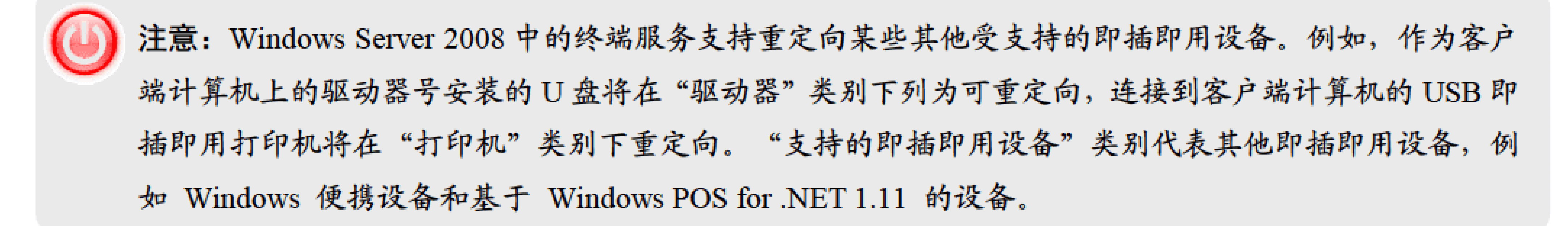


图 12-46 禁用重定向

可以使用终端服务器上的连接指定用户可在远程会话中访问的本地设备和资源。可以启用或禁用下列资源的重定向。

- 驱动器。
- 打印机。
- LPT 端口。
- COM 端口。
- 剪贴板。
- 音频。
- 支持的即插即用设备。
- 默认为主客户端打印机。


注意：Windows Server 2008 中的终端服务支持重定向某些其他受支持的即插即用设备。例如，作为客户端计算机上的驱动器号安装的 U 盘将在“驱动器”类别下列为可重定向，连接到客户端计算机的 USB 即插即用打印机将在“打印机”类别下重定向。“支持的即插即用设备”类别代表其他即插即用设备，例如 Windows 便携设备和基于 Windows POS for .NET 1.11 的设备。

例如，如果禁用了剪贴板的重定向，使用此连接远程连接到终端服务器的用户将无法在远程会话中重定向其剪贴板，即使在远程桌面连接的“选项”下选中了“客户端设置”选项卡中的“剪贴板”复选框也是如此。如果在终端服务器上启用了某个本地设备或资源的重定向，用户仍必须在远程桌面连接的“选项”下的“客户端设置”选项卡中进行相应的设置，指定要重定向该类型的本地驱动器或资源。

12.4.8 配置终端服务会话的超时设置和重新连接设置

默认情况下，终端服务使用用户不必注销并结束会话，即可与远程会话断开。会话处于断开状态时，即使用户不再主动连接，正在运行的程序仍会保持活动状态。

可以限制会话在服务器上保持活动、断开和空闲(没有用户输入)状态的时间。由于在终端服务器上保持无限期运行的会话会继续占用系统资源，所以这样做很有用。

如果按连接配置超时设置和重新连接设置，将影响使用该连接的所有会话。

如图 12-47 所示，可以使用终端服务对“本地用户和组”管理单元或“Active Directory 用户和计算机”管理单元的扩展，按用户配置超时设置和重新连接设置。

使用“终端服务配置”配置的超时设置和重新连接设置将优先于已为特定用户账户配置的超时设置和重新连接设置。

可以在终端服务配置中配置下列超时设置和重新连接设置。

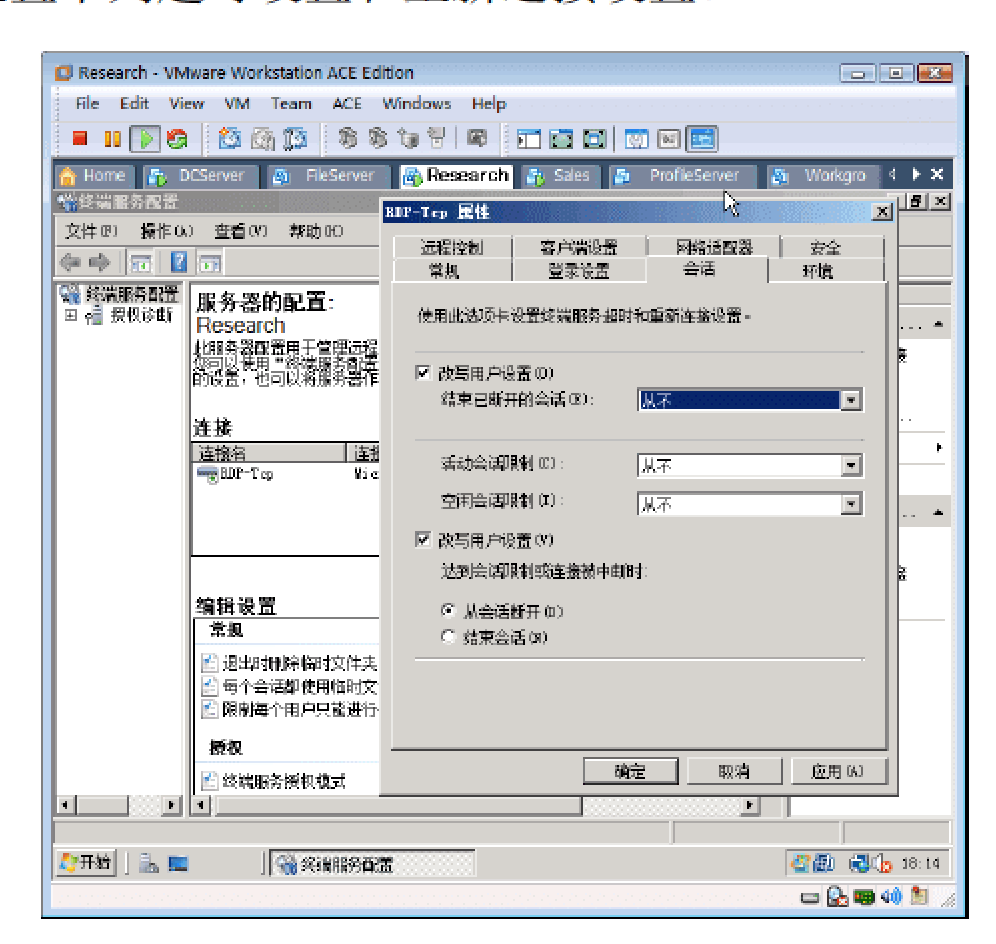


图 12-47 设置会话选项

- 结束已断开的会话：指定已断开的用户会话在终端服务器上保持活动状态的最长时间。如果指定“从不”，用户已断开的会话将无限期保持活动状态。
  会话处于断开状态时，即使用户不再主动连接，正在运行的程序仍会保持活动状态。
- 活动会话限制：指定在会话自动断开或结束之前，用户的终端服务会话可以保持活动状态的最长时间。用户在终端服务会话断开或结束之前两分钟收到警告，使用户可以保存打开的文件并关闭程序。
- 空闲会话限制：指定在会话自动断开或结束之前，活动终端服务会话可以保持空闲状态(没有用户输入)的最长时间。用户在会话断开或结束之前两分钟收到警告，使用户可以按某个键或移动光标来保持会话处于活动状态。
- 达到会话限制或连接被中断时：指定在达到活动会话限制或空闲会话限制时，断开还是结束用户的终端服务会话。如果断开用户会话，即使用户不再主动连接，用户正在运行的程序仍会保持活动状态。如果结束用户会话，用户将需要与终端服务器建立新的终端服务会话。

12.5　终端服务器概述

远程桌面是用来远程管理服务器的，最多只能连接两个会话。如果想让更多的用户连接到服务器，使用安装在服务器上的程序，必须在服务器上安装终端服务，并由终端服务器授权为使用终端服务的用户或设备授权，需要购买终端服务器授权许可。

12.5.1　什么是终端服务

如图 12-48 所示，通过 Windows Server 2008 中的“终端服务”服务器角色提供的技术，用户可以访问终端服务器上安装的基于 Windows 的程序或访问完整的 Windows 桌面。使用终端服务，用户可以在企业网络内部或通过 Internet 访问终端服务器。用户可以连接到终端服务器(Terminal Server)来运行程序，保存文件，以及使用该服务器上的网络资源。用户可以使用远程桌面连接或 RemoteApp 程序访问终端服务器。

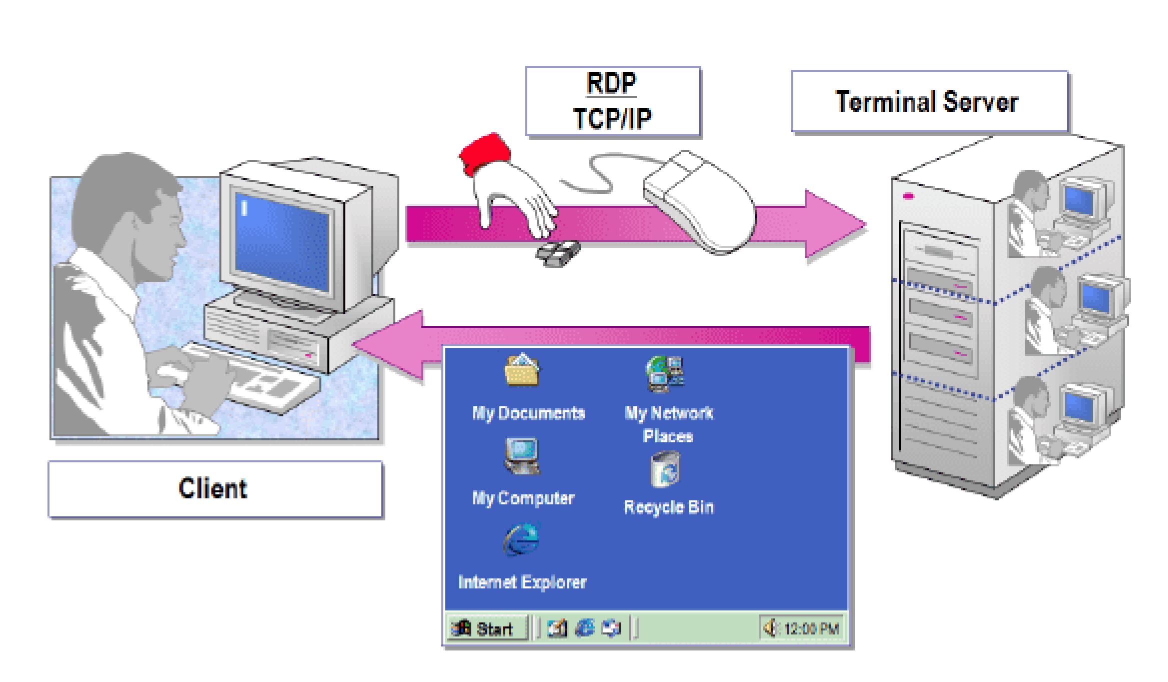


图 12-48　终端服务

终端服务可使用户在企业环境中有效地部署和维护软件。可以很容易从中心位置部署程序。由于将程序安装在终端服务器上，而不是安装在客户端计算机上，所以，更容易升级和维护程序。

用户访问终端服务器上的某个程序时，该程序的执行在服务器上进行，只有键盘、鼠标和显示器的信息才通过网络传输。每个用户只能看到自己的会话。服务器操作系统透明地管理会话，与任何其他客户端会话无关。

12.5.2　为什么使用终端服务

如果在终端服务器上(而不是在每台设备上)部署程序，则可以带来诸多好处。具体如下。

- 可以快速地将基于 Windows 的程序部署到整个企业中的计算设备上。在程序经常需要更新、很少使用或难以管理的情况下，终端服务尤其有用。
- 终端服务可以明显减少访问远程应用程序所需的网络带宽量。
- 终端服务有助于提高用户的工作效率。用户可以从家用计算机、展台、低能耗硬件等设备以及非 Windows 操作系统访问终端服务器上运行的程序。
- 对于需要访问中心数据存储的分支机构工作人员来说，终端服务可提供更好的程序性能。有时，

数据密集型程序没有针对低速连接进行优化的客户端/服务器协议。较典型的广域网连接而言，此类通过终端服务连接运行的程序性能会更好。

12.5.3 终端服务角色服务

终端服务是由多个子组件(称为“角色服务”)组成的服务器角色。在 Windows Server 2008 中，终端服务由下列角色服务组成。

- 终端服务器：“终端服务器”角色服务使服务器可以托管基于 Windows 的程序或完整的 Windows 桌面。用户可以连接到终端服务器来运行程序，保存文件，以及使用该服务器上的网络资源。
- TS Web Access：Terminal Services Web Access (TS Web Access) 使用户可以通过网站访问 RemoteApp™ 程序以及远程桌面与终端服务器的连接。
- TS Licensing：终端服务授权(TS 授权) 管理每个设备或用户连接到终端服务器所需的终端服务客户端访问许可证 (TS CAL)。使用 TS 授权在终端服务许可证服务器上安装、颁发 TS CAL 并监视其可用性。
- TS Gateway：终端服务网关(TS 网关) 使授权远程用户可以从任何连接到 Internet 的设备连接到内部公司网络上的资源。
- TS Session Broker：Terminal Services Session Broker (TS Session Broker) 支持在服务器场中的终端服务器之间进行会话负载平衡，并支持重新连接到负载平衡终端服务器场中的现有会话。

12.5.4 终端服务远程应用程序(TS RemoteApp)

RemoteApp 程序是通过终端服务远程访问的程序，它们的行为就好像运行在最终用户的本地计算机上一样。用户可以将 RemoteApp 程序与本地程序并排运行。如果用户从同一台终端服务器运行多个 RemoteApp 程序，RemoteApp 程序将共享同一个终端服务会话。通过此功能可以节省用户会话，并且可以更快地连接到同一台服务器上的每个其他 RemoteApp 程序。

通过使用 TS RemoteApp Manager，可以创建 Windows 安装程序包(.msi 程序包)或.rdp 文件，然后在整个组织中分发程序包。或者，如果希望用户通过 Web 访问 RemoteApp 程序，可以使用 TS Web Access 将 RemoteApp 程序部署到网站上。

为什么使用 TS RemoteApp

在许多情况下 TS RemoteApp 可以降低复杂程度并减少管理开销，例如下面几种情况。

- 分支机构，其本地 IT 支持和网络带宽可能有限。
- 用户需要远程访问应用程序的情况。
- 部署行业 (LOB) 应用程序，尤其是自定义 LOB 应用程序。
- 没有为用户分配计算机的环境，例如“公用办公桌”或“旅馆式办公”工作空间。
- 部署某个应用程序的多个版本时，尤其是当在本地安装多个版本可能会造成冲突时。

12.5.5 TS Web Access

通过 TS Web Access，用户可以从 Web 浏览器使用 RemoteApp 程序以及远程桌面与终端服务器的连接。通过 TS Web Access，用户可以通过访问网站(从 Internet 或 Intranet)访问可用 RemoteApp 程序

的列表。在启动 RemoteApp 程序时，将在托管 RemoteApp 程序的终端服务器上启动终端服务会话。

在部署 TS Web Access 时，可以指定充当数据源的终端服务器，以填充网页上出现的 RemoteApp 程序的列表。

12.5.6　TS Licensing

TS 授权管理每个用户或设备连接到终端服务器所需的 TS CAL。使用 TS 授权在终端服务许可证服务器上安装、颁发 TS CAL 并监视其可用性。

若要使用终端服务，必须至少拥有一台许可证服务器。对于小型部署，可以将“终端服务器”角色服务和 TS 授权角色服务安装在同一台计算机上。对于较大型的部署，建议将 TS 授权角色服务与“终端服务器”角色服务安装在不同的计算机上。

只有正确地配置了 TS 授权，终端服务器才能继续接受来自客户端的连接。

12.5.7　终端服务网关

任意地点的安全访问：很多时候出差在外的员工需要应用某个特定的应用软件，如公司定制的财务软件等，这时候员工可以通过手机、笔记本等移动设备，在任意地点连接公司终端服务器进行应用。如在 Windows Server 2008 中，用户可以利用终端服务中的 TS Web Access 功能，没必要连接 VPN，仅仅通过 Web 方式即可访问企业终端服务器，并且可以获得良好的用户体验。如图 12-49 所示，Windows Server 2008 中的终端服务具有网关功能(TS Gateway)，可以裁决用户是否满足连接条件，并且可以确定用户可以连接哪些终端服务器，保证了安全性。

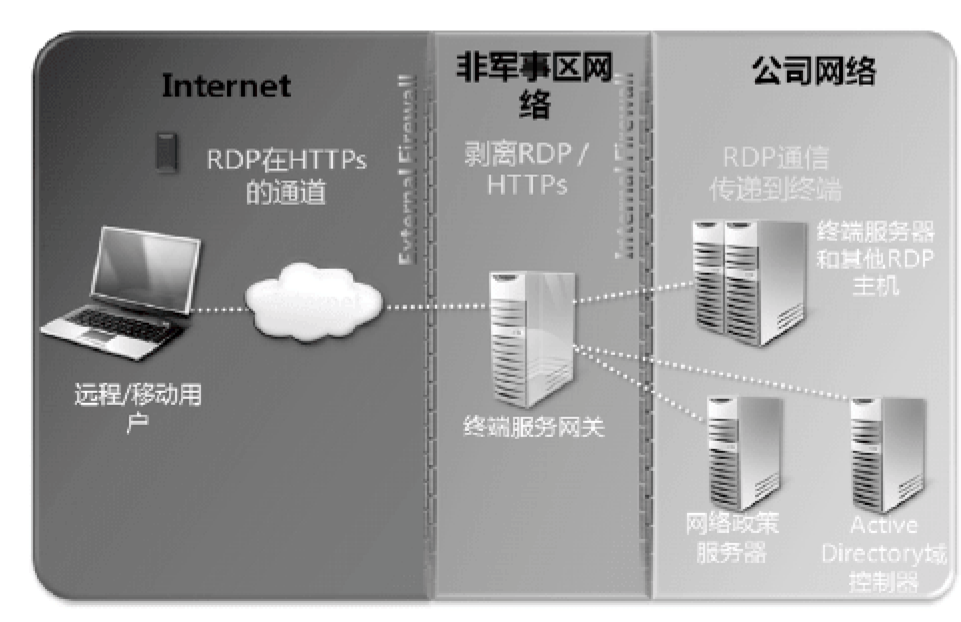


图 12-49　终端服务器网关

终端服务网关(TS 网关)是这样一种类型的网关，它允许授权用户使用 Internet 连接从任何计算机连接到企业网络上的远程计算机。TS 网关使用远程桌面协议 (RDP) 和 HTTPS 帮助创建更安全的加密连接。

在远程桌面连接的早期版本中，人们无法跨过防火墙和网络地址转换器连接到远程计算机，原因是为增强网络的安全性，通常将 3389 端口——用于远程桌面连接的端口——堵塞。但是，TS 网关服务器使用 443 端口，通过安全套接字层 (SSL) 隧道来传输数据。

TS 网关服务器具有以下优点。

- 支持远程用户通过 Internet 安全连接到企业网络上的资源，消除了 VPN 连接的复杂性问题。

- 充分利用 HTTPS 协议的安全性与可用性，实现了无须客户端配置即可提供终端服务。
- 提供全面的安全配置模型，使管理员能控制对网络上特定资源的访问。
- 使用户能通过不同防火墙和网络地址转换器 (NAT) 远程连接到终端服务器与远程工作站上。
- 提供一种更安全的模式，使用户通过 VPN 只能访问指定的服务器与工作站，而不是整个企业网络。
- TS 网关通过使用 HTTP Secure Sockets Layer (SSL)通道传输所有 RDP 流量(通常会通过端口 3389 发送)至端口 443。这意味着所有用户客户端电脑以及 TS 网关的流量都将在经过 Internet 传输时进行加密。

12.5.8 TS Session Broker

TS Session Broker(终端服务会话中介器)在负载平衡的终端服务器场中跟踪用户会话。TS Session Broker 数据库存储会话状态信息，包括会话 ID、会话关联的用户名以及每个会话所在的服务器的名称。拥有现有会话的用户连接到负载平衡服务器场中的终端服务器时，TS Session Broker 将用户重定向到其会话所在的终端服务器。这样可以阻止用户连接到服务器场中的其他服务器并启动新会话。

如果启用了 TS Session Broker 负载平衡功能，TS Session Broker 还跟踪服务器场中每台终端服务器上的用户会话数，并将没有现有会话的用户重定向到会话数最少的服务器。通过此功能，可以将会话负载在负载平衡终端服务器场中的服务器之间均匀分配。

12.6 安装和配置终端服务

12.6.1 安装终端服务授权

在 DCServer 安装终端服务器授权，给域中的终端服务器分发终端服务器许可。

① 以域管理员账号登录 DCServer，如图 12-50 所示，打开服务器管理器，单击“添加角色”按钮。

② 在出现的“开始之前”界面中，单击“下一步”按钮。

③ 如图 12-51 所示，在“选择服务器角色”界面中，选中“终端服务”复选框，单击“下一步”按钮。

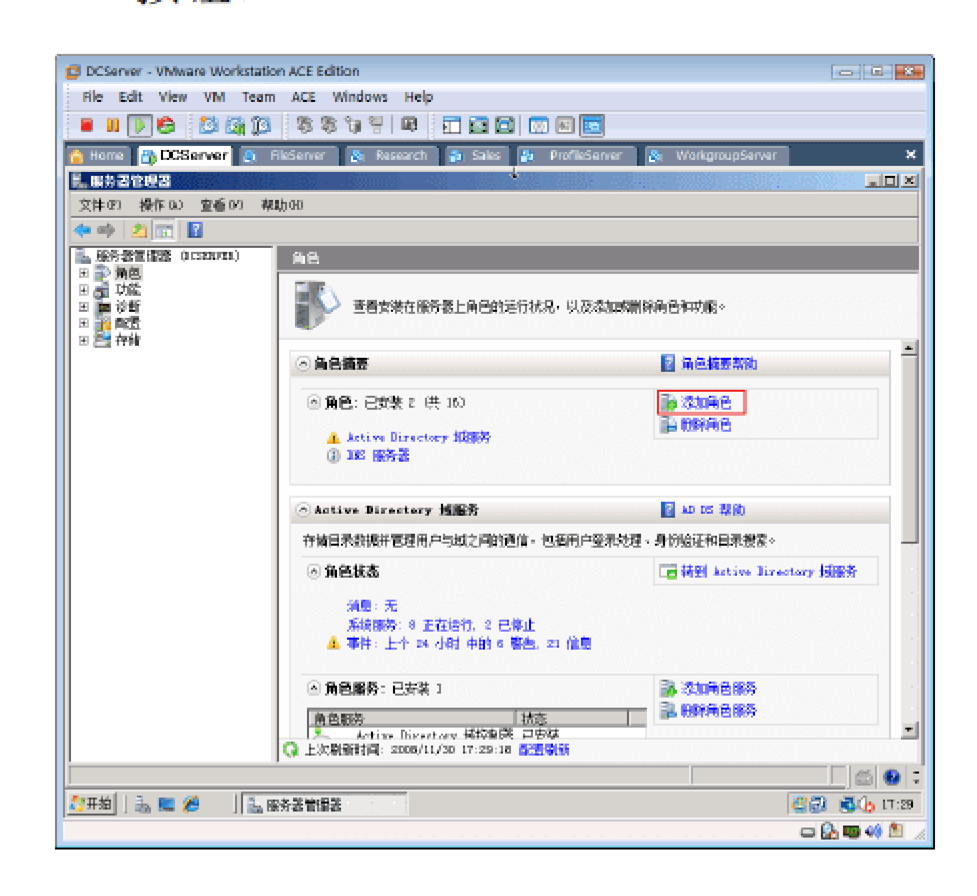


图 12-50 添加角色

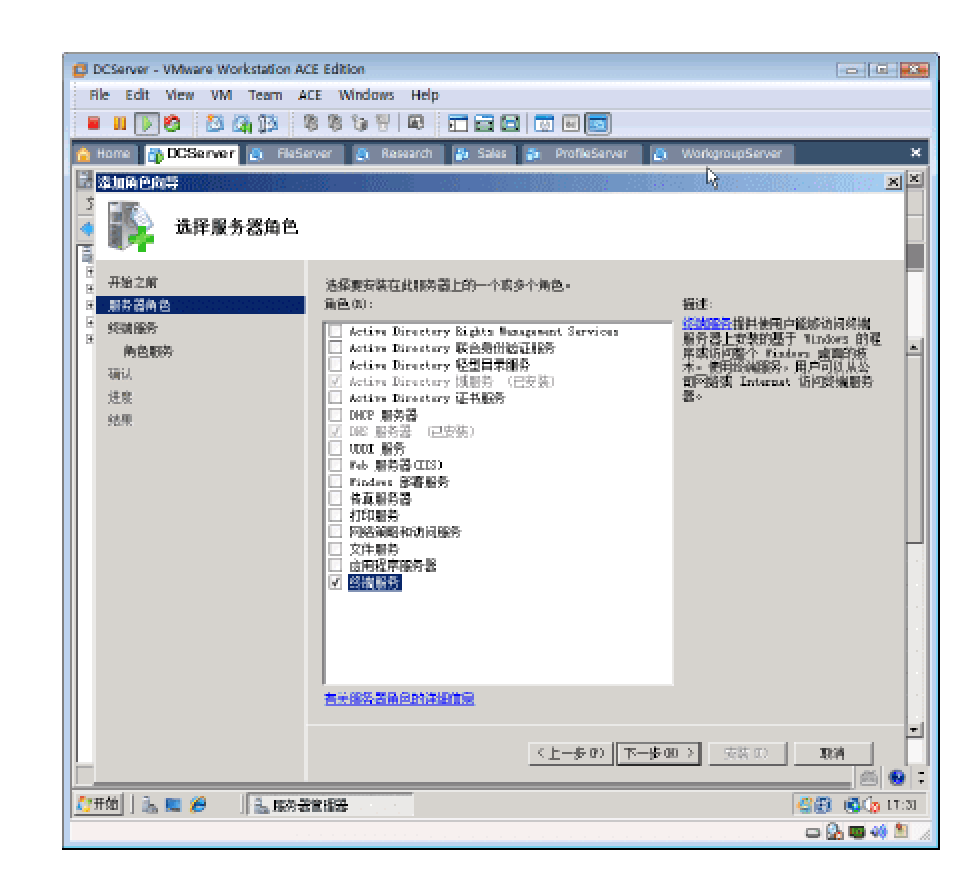


图 12-51 选择角色

④　在出现的“终端服务介绍”界面中，单击“下一步”按钮。

⑤　如图 12-52 所示，在出现的“选择角色服务”界面中，选中“TS 授权”复选框，单击“下一步”按钮。

⑥　如图 12-53 所示，在“为 TS 授权配置搜索范围”界面中，选中“此域”单选按钮，单击“下一步”按钮。

⑦　在出现的“确认”对话框中，单击“下一步”按钮，完成角色添加。

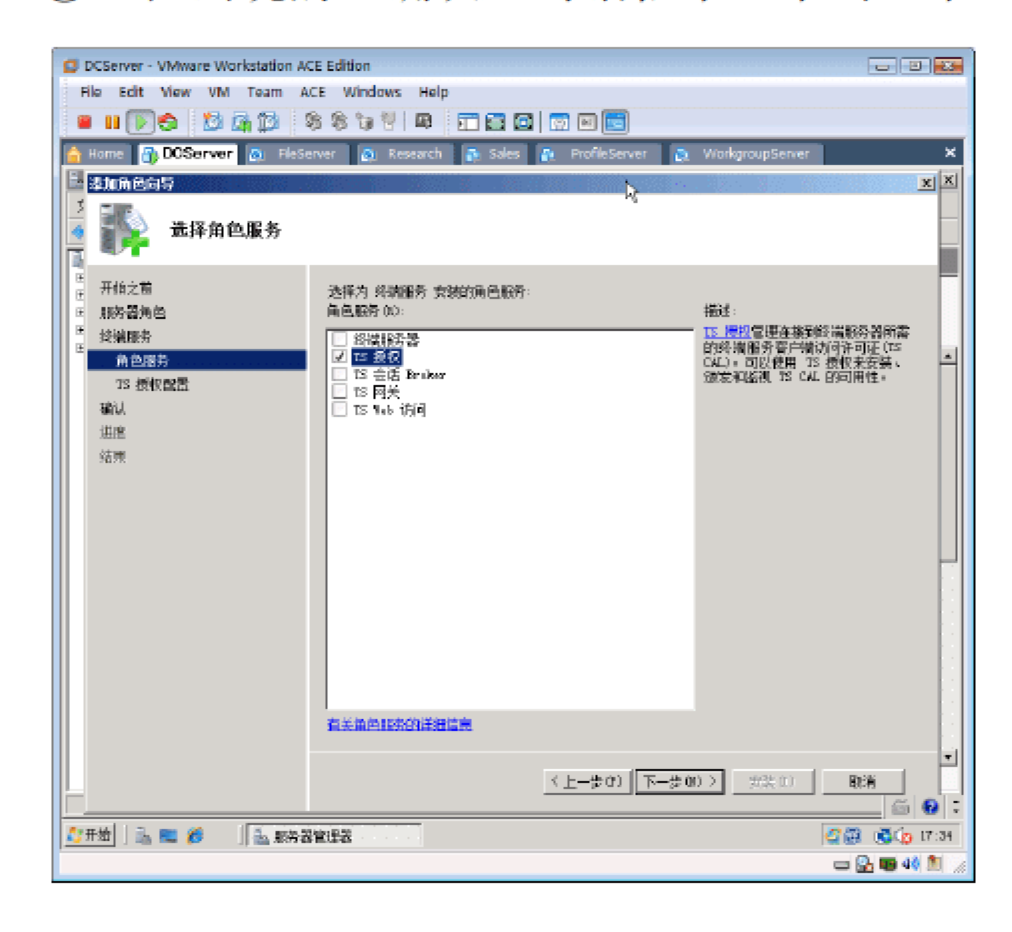




图 12-52　选择角色服务

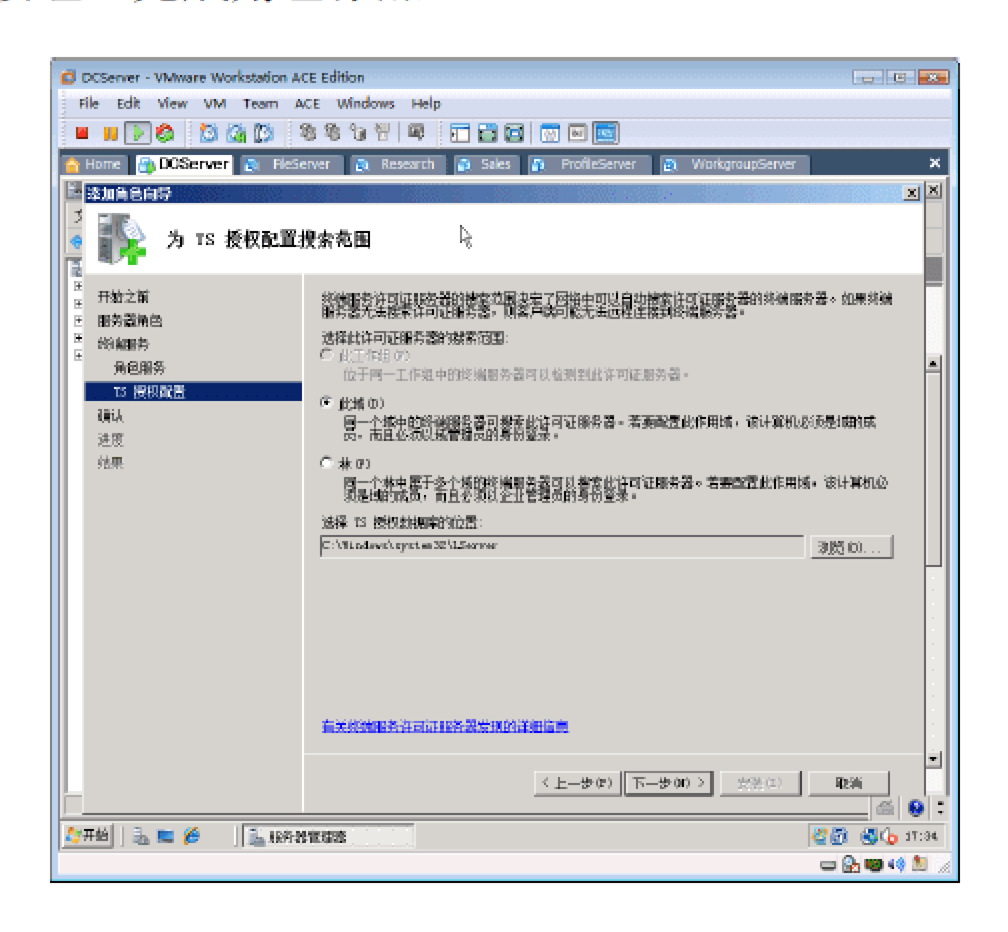


图 12-53　选择 TS 授权配置搜索范围

12.6.2　激活终端服务授权

必须激活许可证服务器，才能验证该许可证服务器并允许其颁发终端服务客户端访问许可证 (TS CAL)。可以使用 TS 授权管理器工具中的服务器激活向导来激活许可证服务器。

如果没有激活许可证服务器，许可证服务器只能颁发临时 TS 每设备 CAL(有效期为 90 天)或 TS 每用户 CAL。

可以通过下列三种方法激活许可证服务器。

- 自动激活终端服务许可证服务器。
- 使用 Web 浏览器激活终端服务许可证服务器。
- 使用电话激活终端服务许可证服务器。

下面介绍自动激活终端服务 DCSERVERTS 授权服务的详细步骤。

①　选择“开始”→“程序”→“管理工具”→“终端服务”→“TS 授权管理器”命令。

②　如图 12-54 所示，右击服务器，从弹出的快捷菜单中选择“激活服务器”命令。

③　如图 12-55 所示，在出现的“服务器激活向导”对话框中，单击“下一步”按钮。

④　如图 12-56 所示，在“连接方法”界面中，选择“自动连接”，单击“下一步”按钮。

⑤　如图 12-57 所示，在“公司信息”界面中，输入公司信息，单击“下一步”按钮。

⑥　如图 12-58 所示，在“公司信息”界面中，继续输入公司信息，单击“下一步”按钮。

⑦　如图 12-59 所示，在“正在完成服务器激活向导”界面中，单击“下一步”按钮。

⑧　如图 12-60 所示，在“欢迎使用许可证安装向导”界面中，单击“下一步”按钮。

⑨　如图 12-61 所示，在“许可证计划”界面中，选择“其他协议”选项，单击“下一步”按钮。

⑩ 如图 12-62 所示，在“许可证计划”界面中，输入协议号码，单击“下一步”按钮。

⑪ 如图 12-63 所示，在“产品版本和许可证类型”界面，产品版本选择 Windows Server 2008，许可证类型选择“Windows Server 2008 TS 每用户 CAL”，输入数量，单击“下一步”按钮。

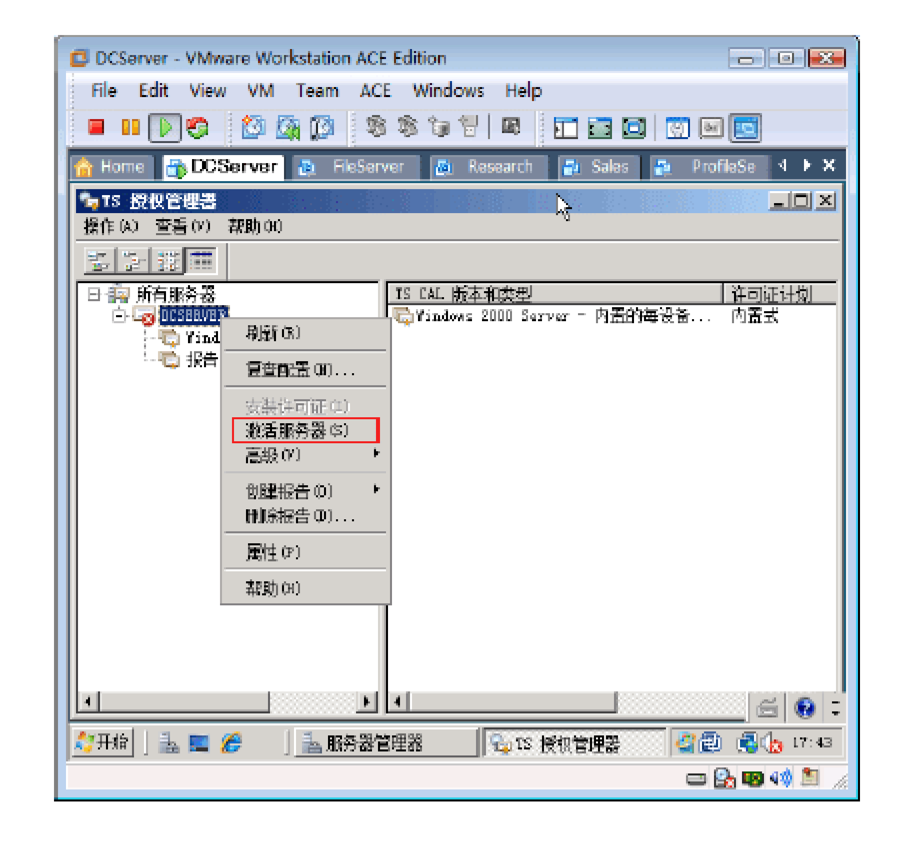


图 12-54　激活服务器

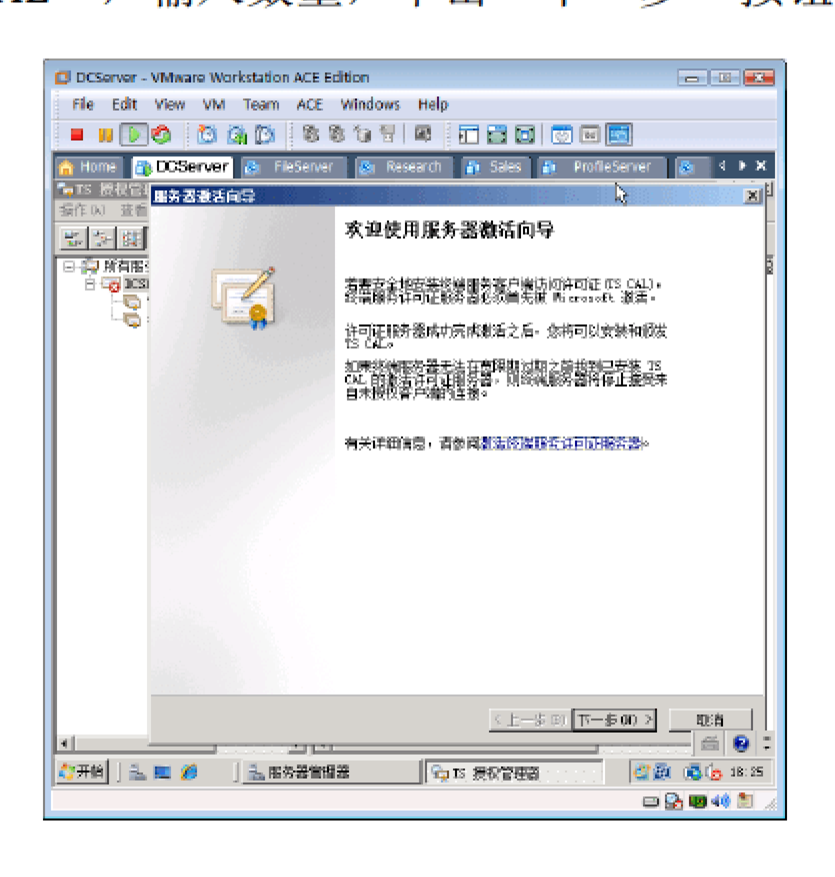


图 12-55　激活服务器向导

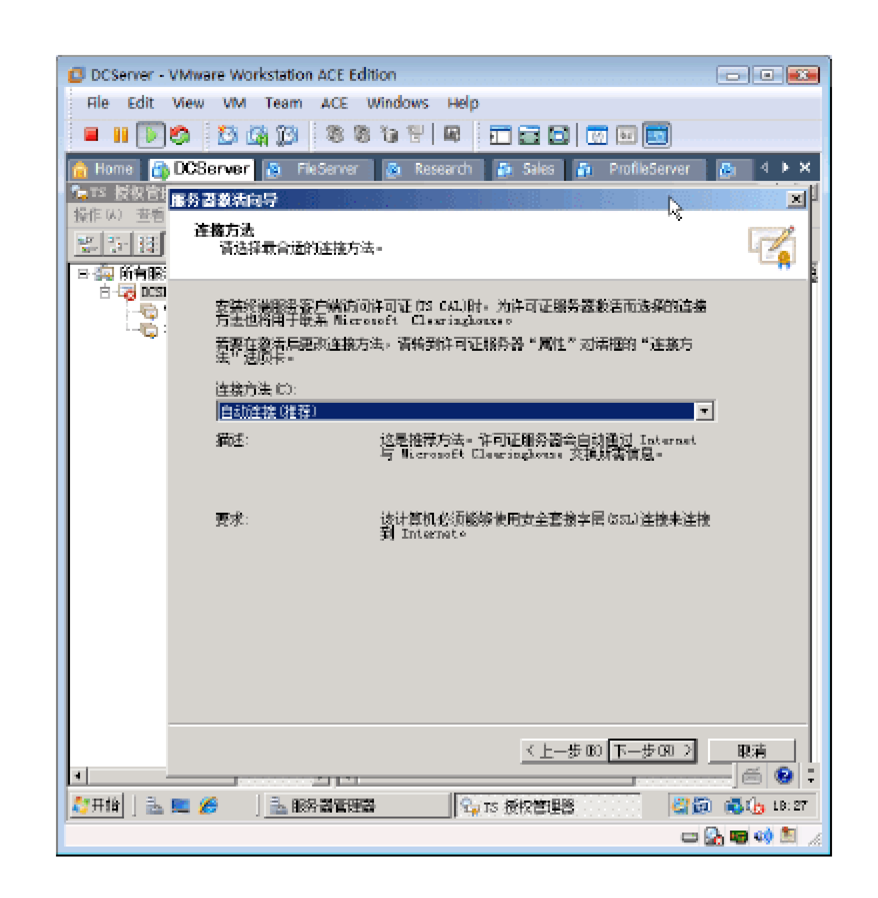


图 12-56　选择连接方法

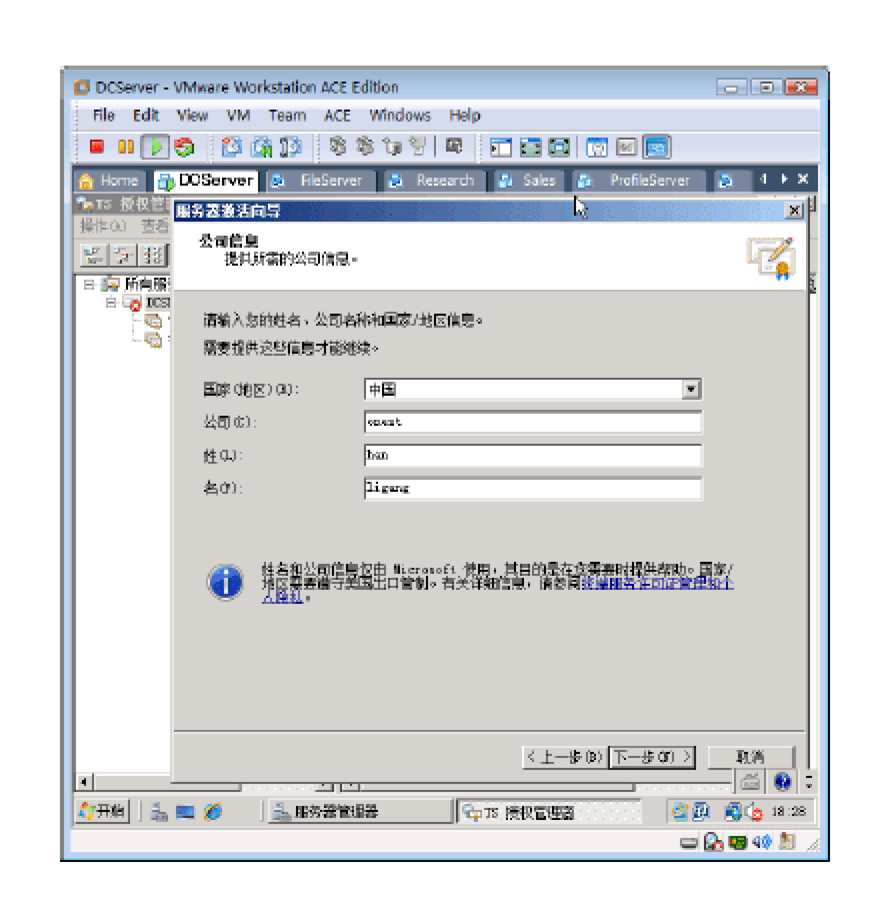


图 12-57　输入公司信息

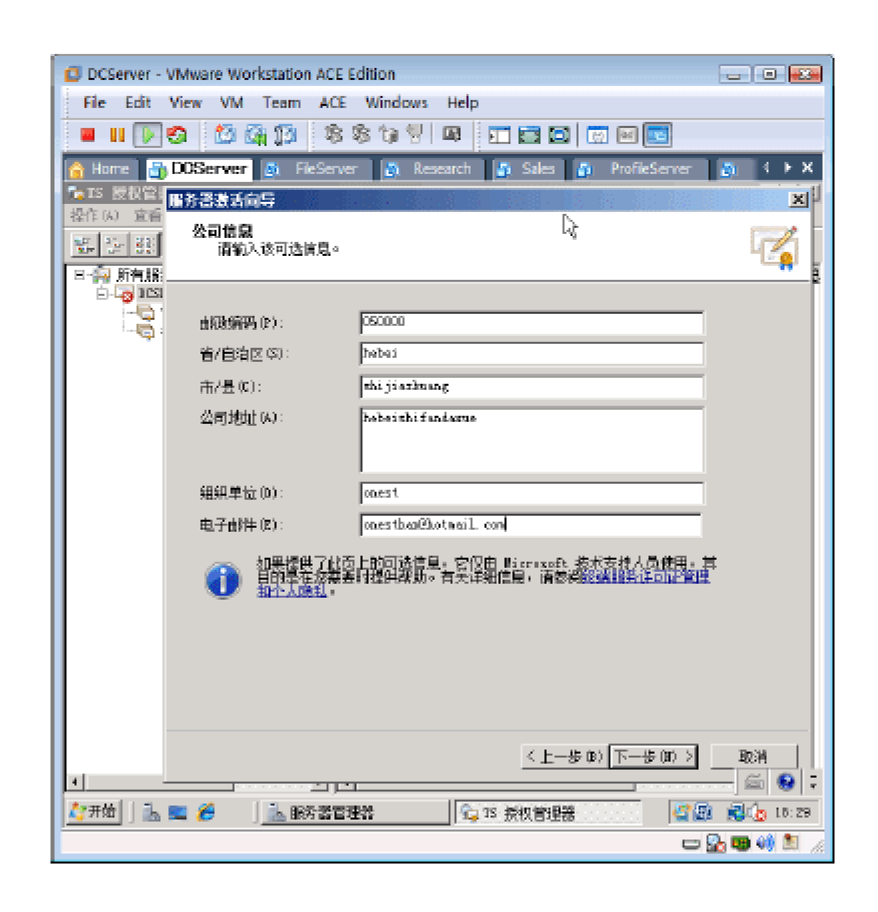


图 12-58　继续输入公司信息

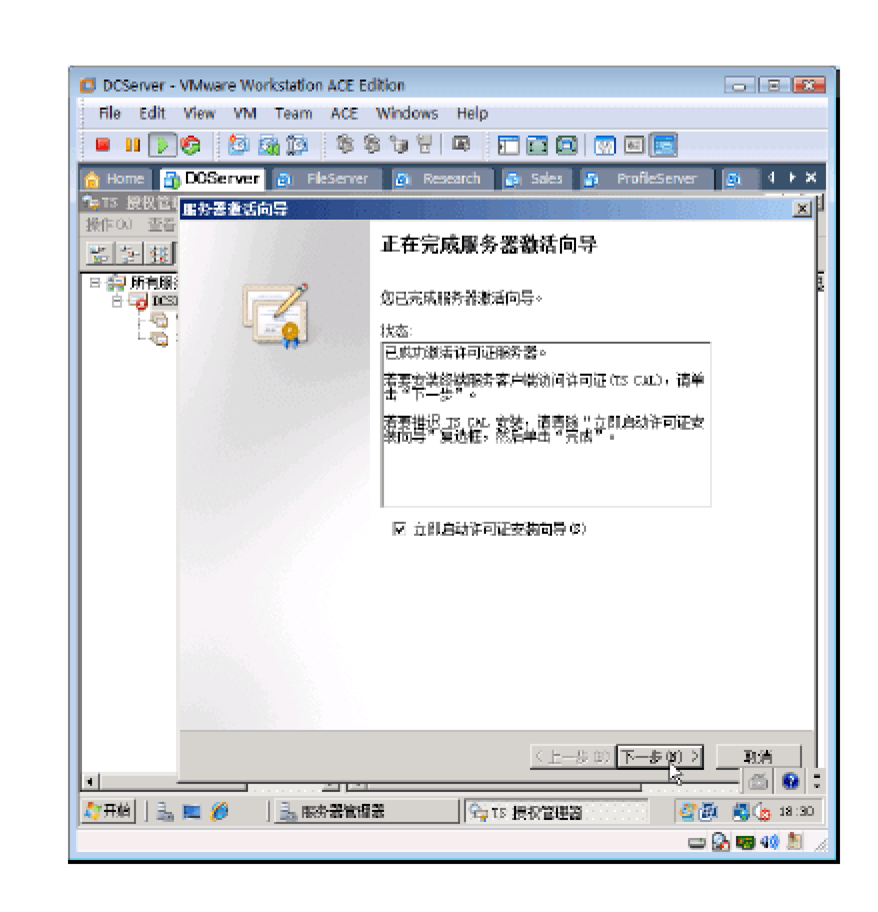


图 12-59　激活向导

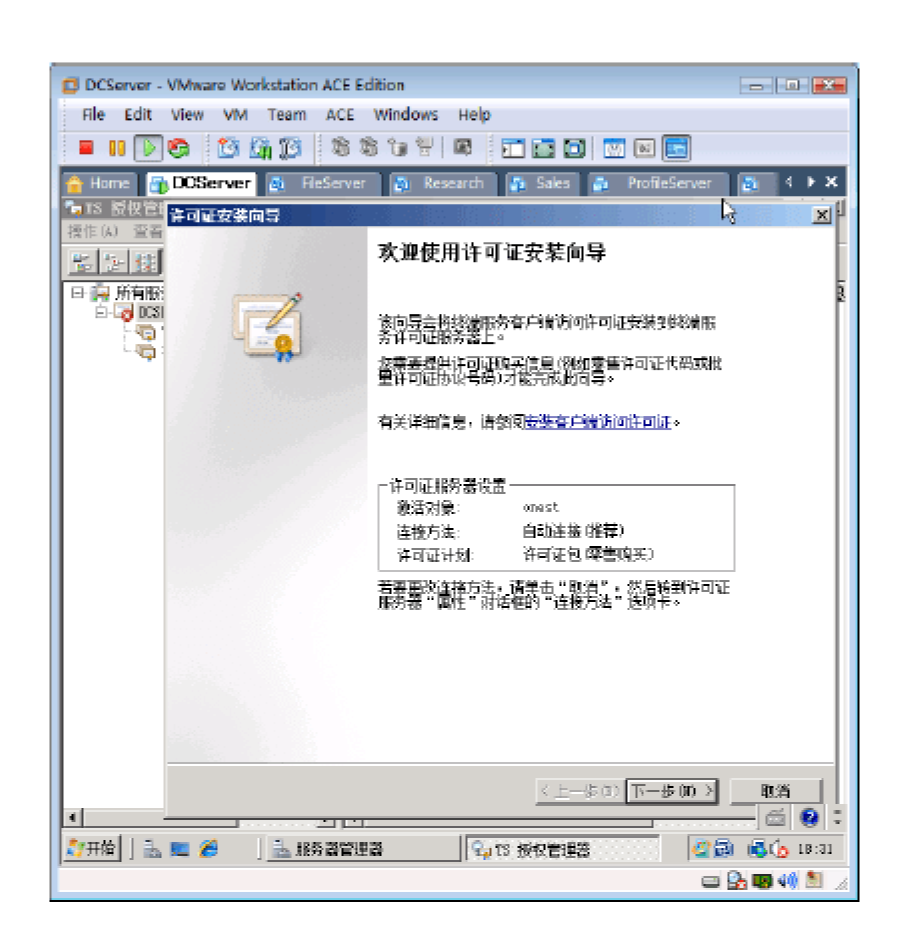


图 12-60　安装向导

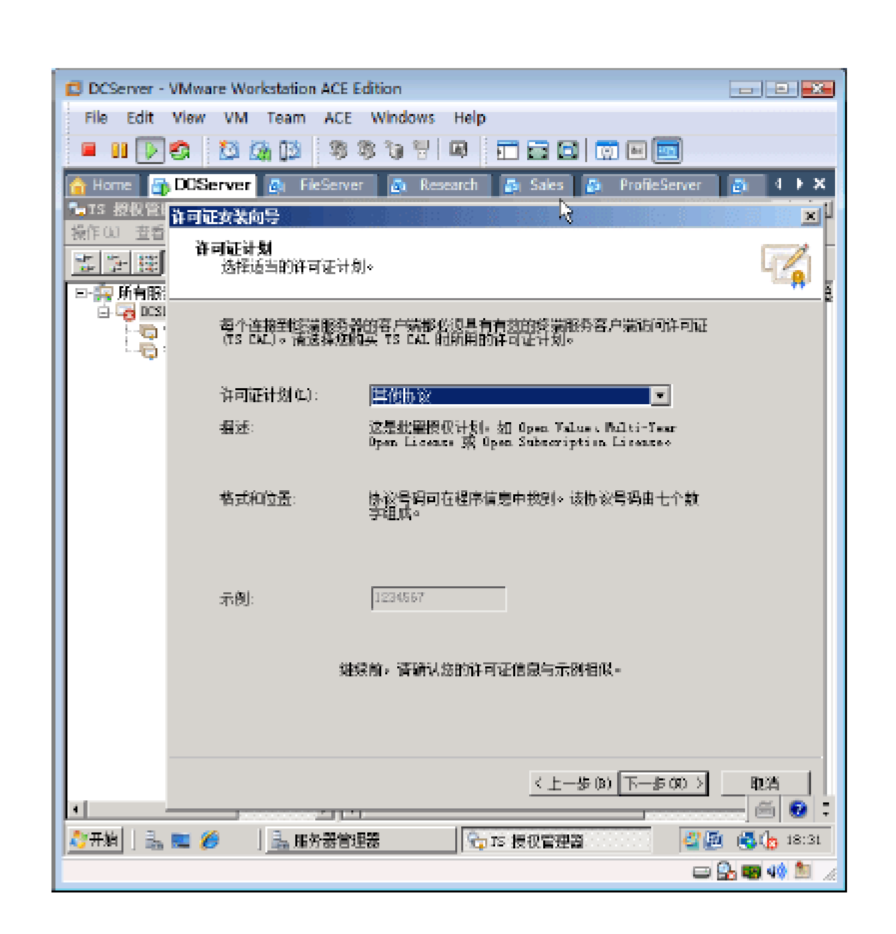


图 12-61　许可证计划

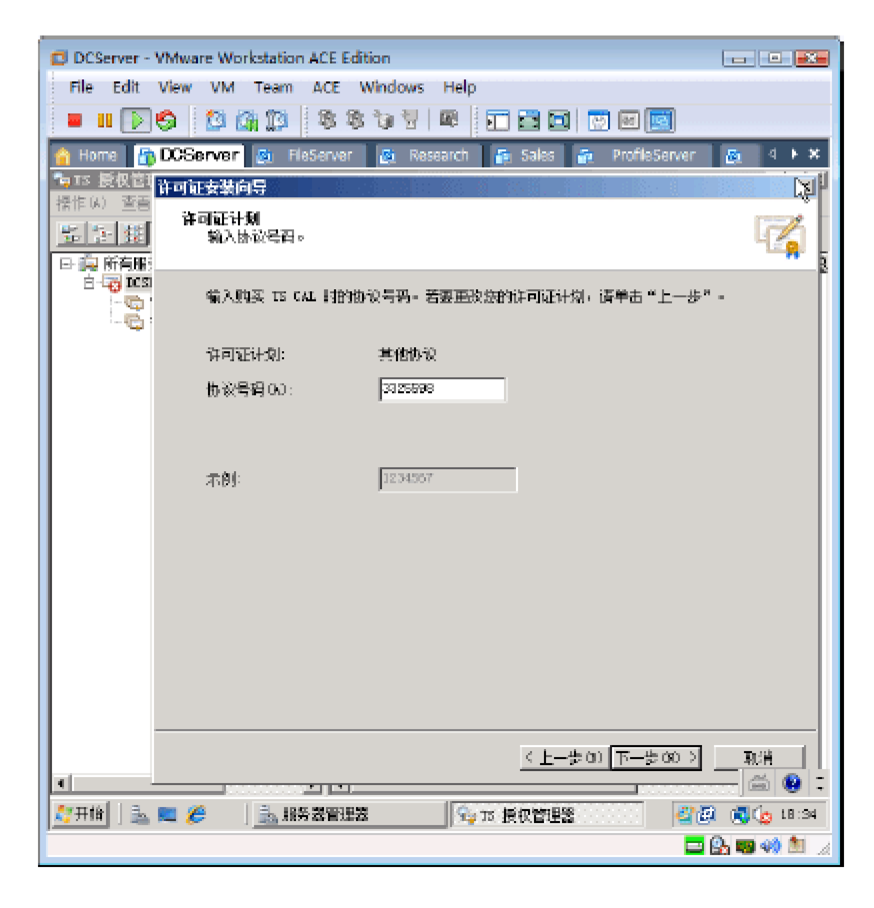


图 12-62　输入协议号码

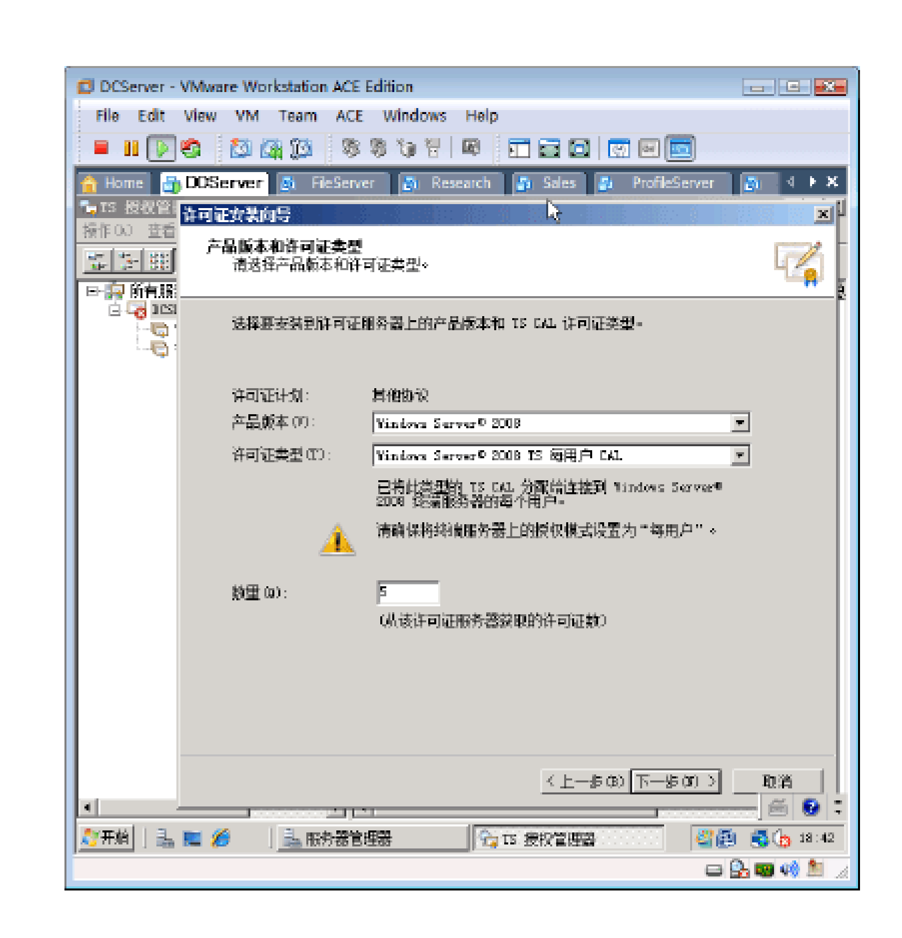


图 12-63　选择产品版本

⑫　如图 12-64 所示，完成后可以看到批量许可证数量为 5。

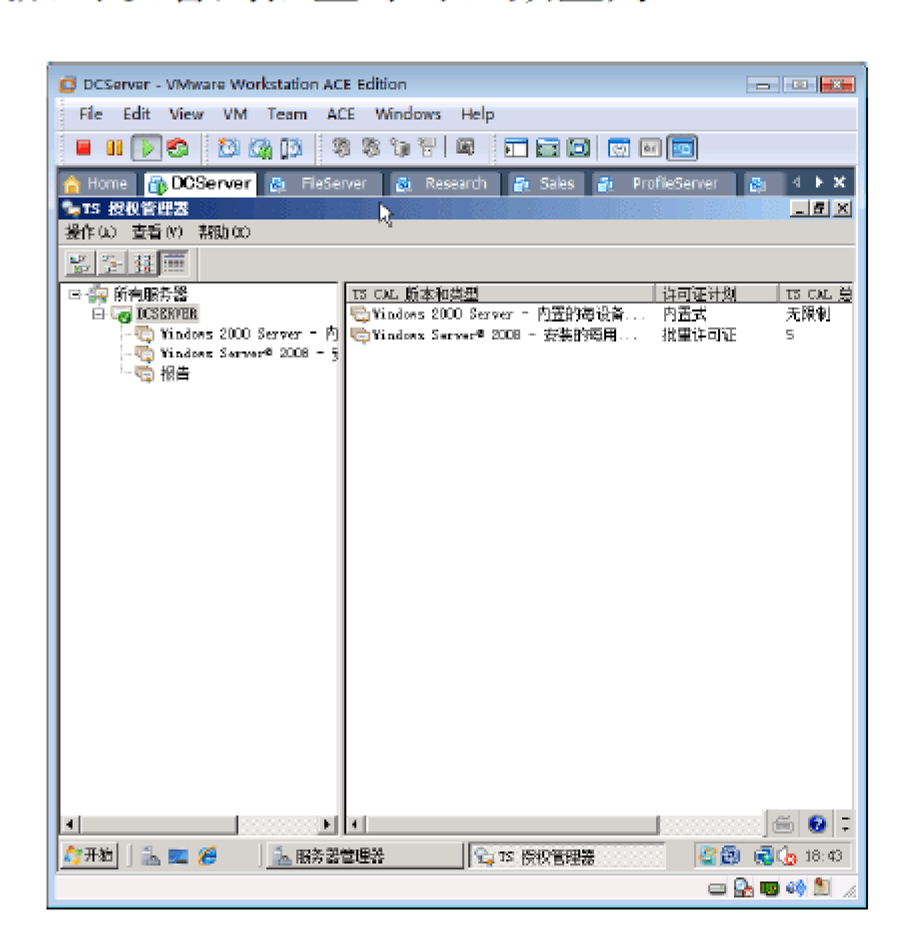


图 12-64　许可证数量

12.6.3　安装终端服务器

可以在 FileServer 计算机安装终端服务，以便用户能够访问其上的应用程序。

① 以域管理员账户登录到 FileServer，打开服务器管理器，单击“添加角色”按钮。

② 如图 12-65 所示，选中“终端服务”复选框，单击“下一步”按钮。

③ 在“终端服务”界面中，单击“下一步”按钮。

④ 如图 12-66 所示，在“选择角色服务”界面中，选中“终端服务器”、“TS 会话 Broker”和“TS Web 访问”复选框，单击“下一步”按钮，在弹出的对话框中，单击“添加必需的角色服务”按钮。

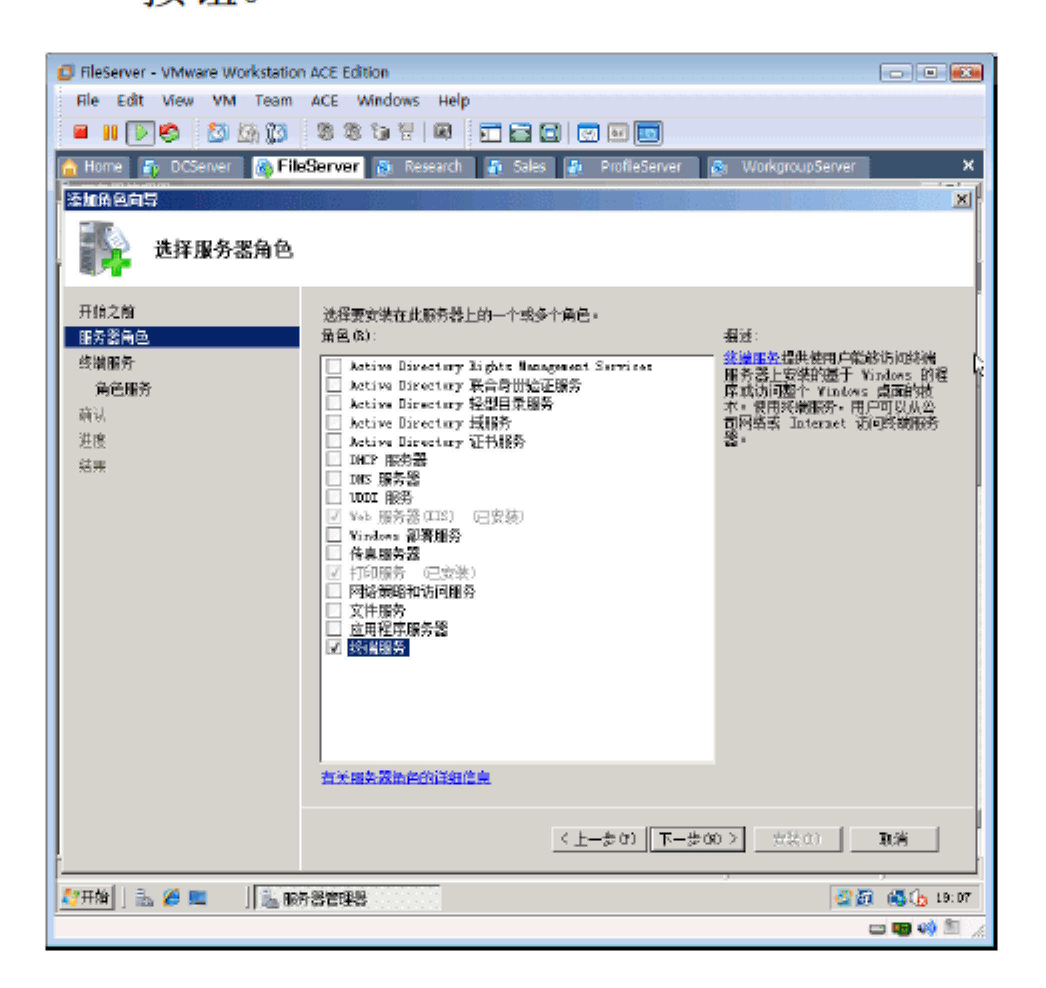


图 12-65　安装终端服务

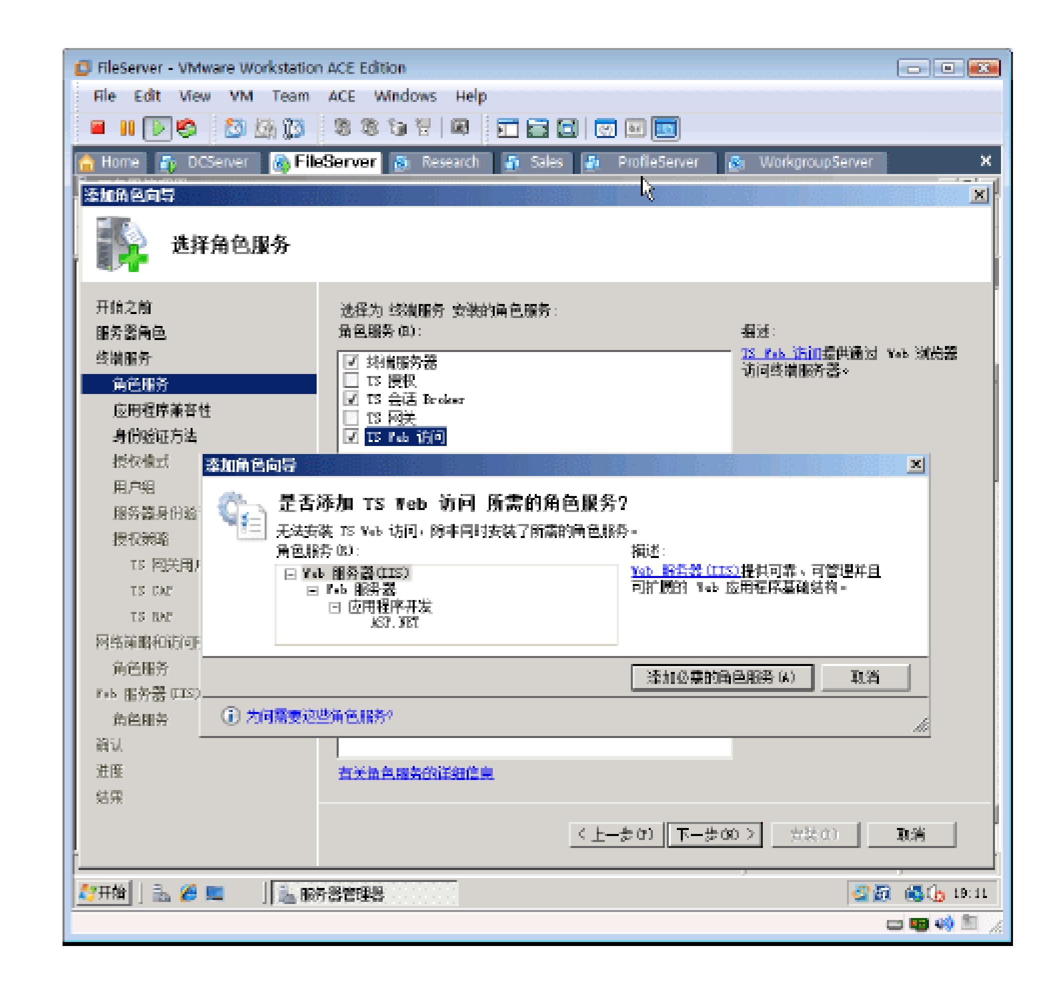


图 12-66　选择角色服务

⑤ 如图 12-67 所示，在“卸载并重新安装兼容的应用程序”界面中，单击“下一步”按钮。

⑥ 如图 12-68 所示，在“指定终端服务器的身份验证方法”界面中，选中“要求使用网络级身份验证”单选按钮，单击“下一步”按钮。

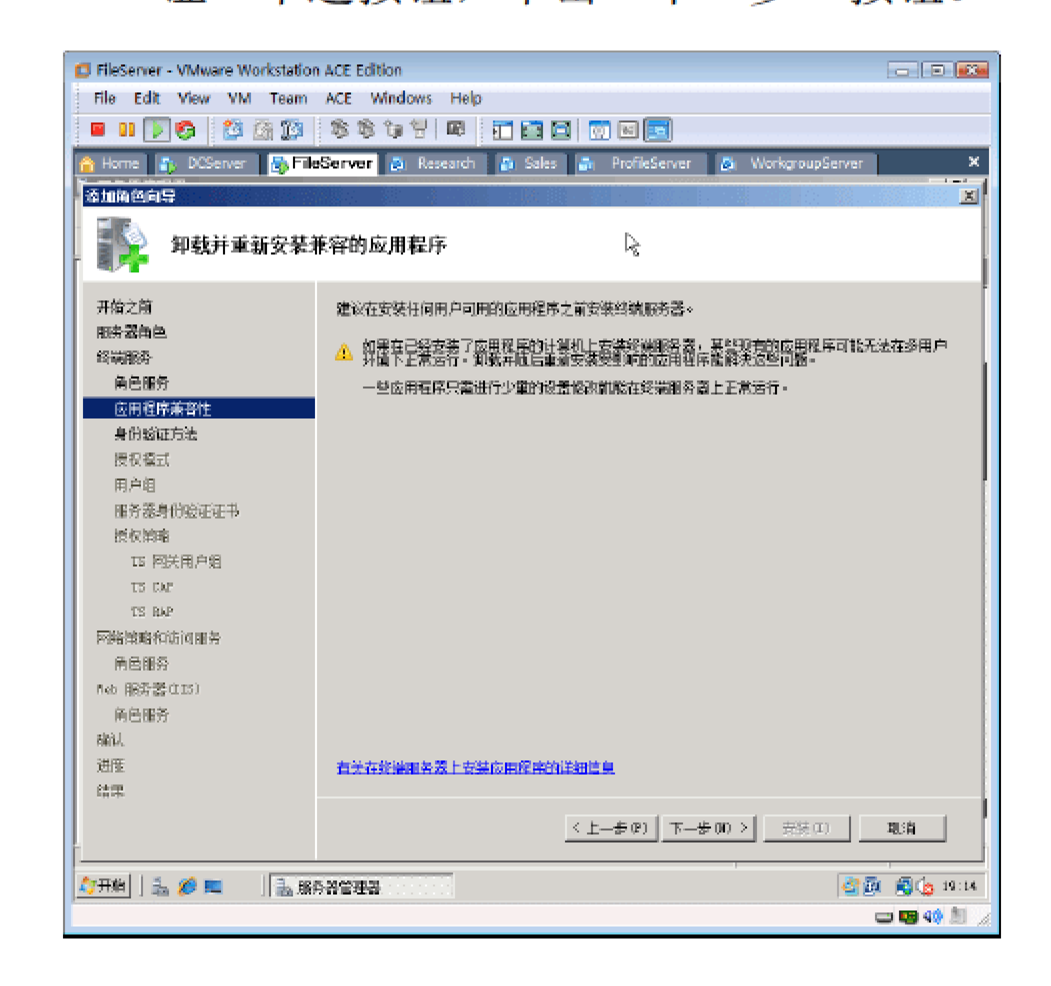


图 12-67　安装向导

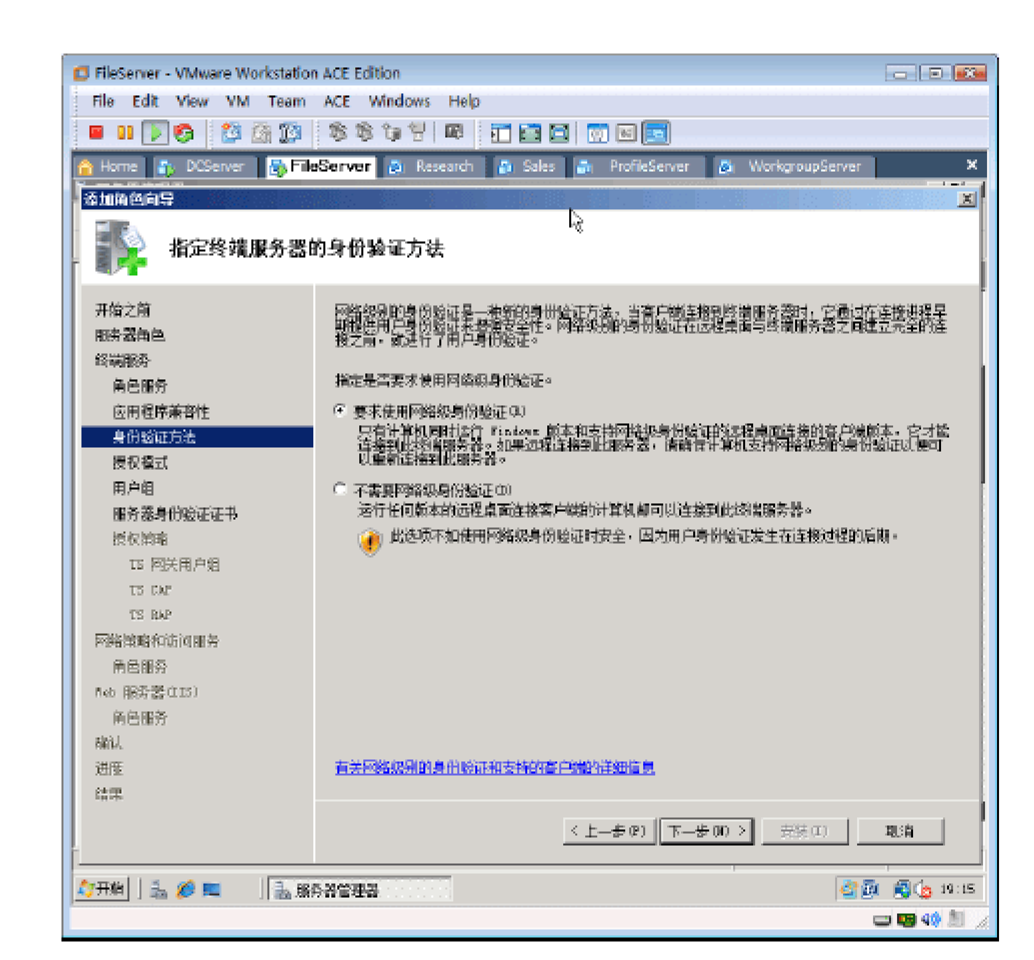


图 12-68　身份验证方法

注意：应先在计算机上安装“终端服务器”角色服务，然后再安装任何希望用户可以使用的程序。如果在已安装了程序的计算机上安装“终端服务器”角色服务，在多用户环境中，某些现有的程序可能无法正常运行。卸载并重新安装受影响的程序可能会解决这些问题。为了确保正确地安装某个应用程序，以便在多用户环境中使用，必须先将终端服务器置于特殊安装模式，然后再在终端服务器上安装该应用程序。此特殊安装模式确保在安装期间创建所需的正确注册表项和.ini 文件，以支持在多用户环境中运行该应用程序。

⑦ 如图 12-69 所示，在出现的“指定授权模式”界面中，选中“每用户”单选按钮，单击“下一步”按钮。

⑧ 如图 12-70 所示，在出现的“选择允许访问此终端服务器的用户组”界面中，单击“下一步”按钮。

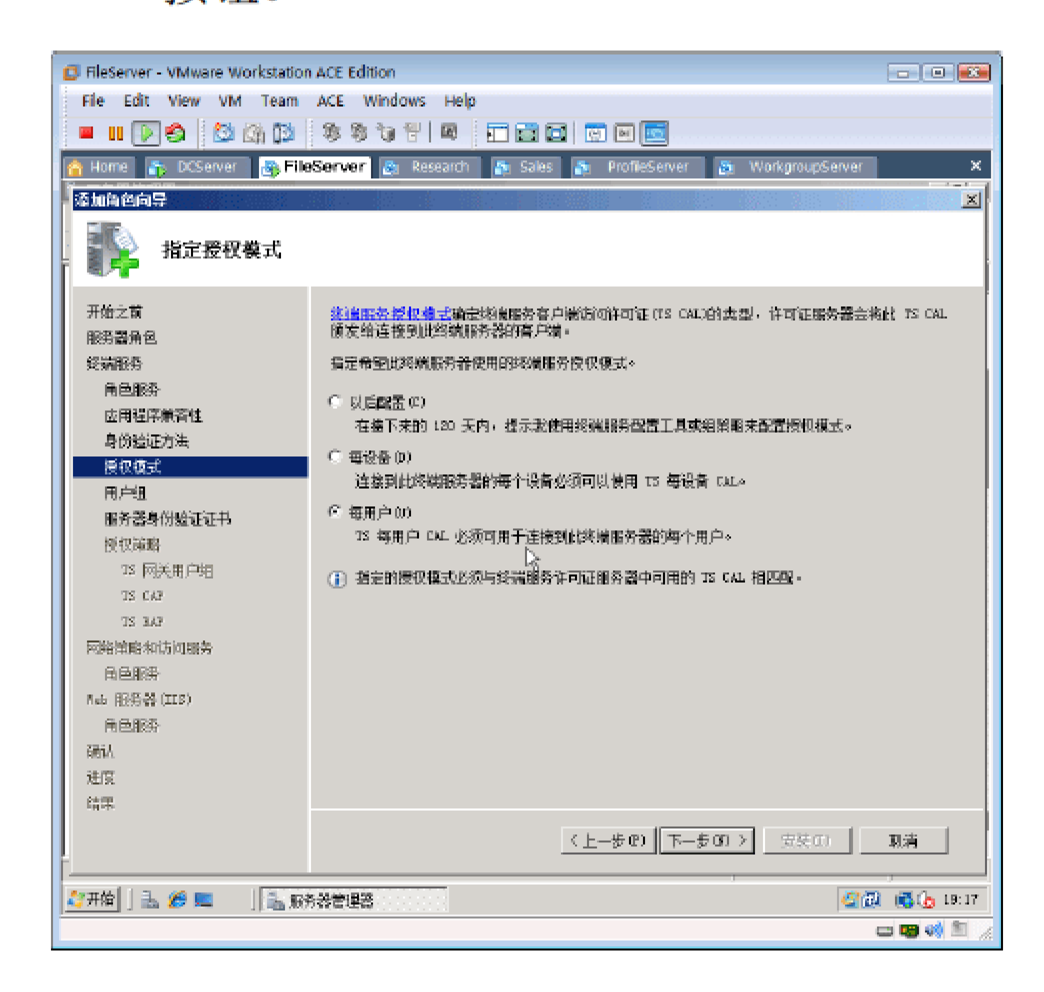


图 12-69　指定授权模式

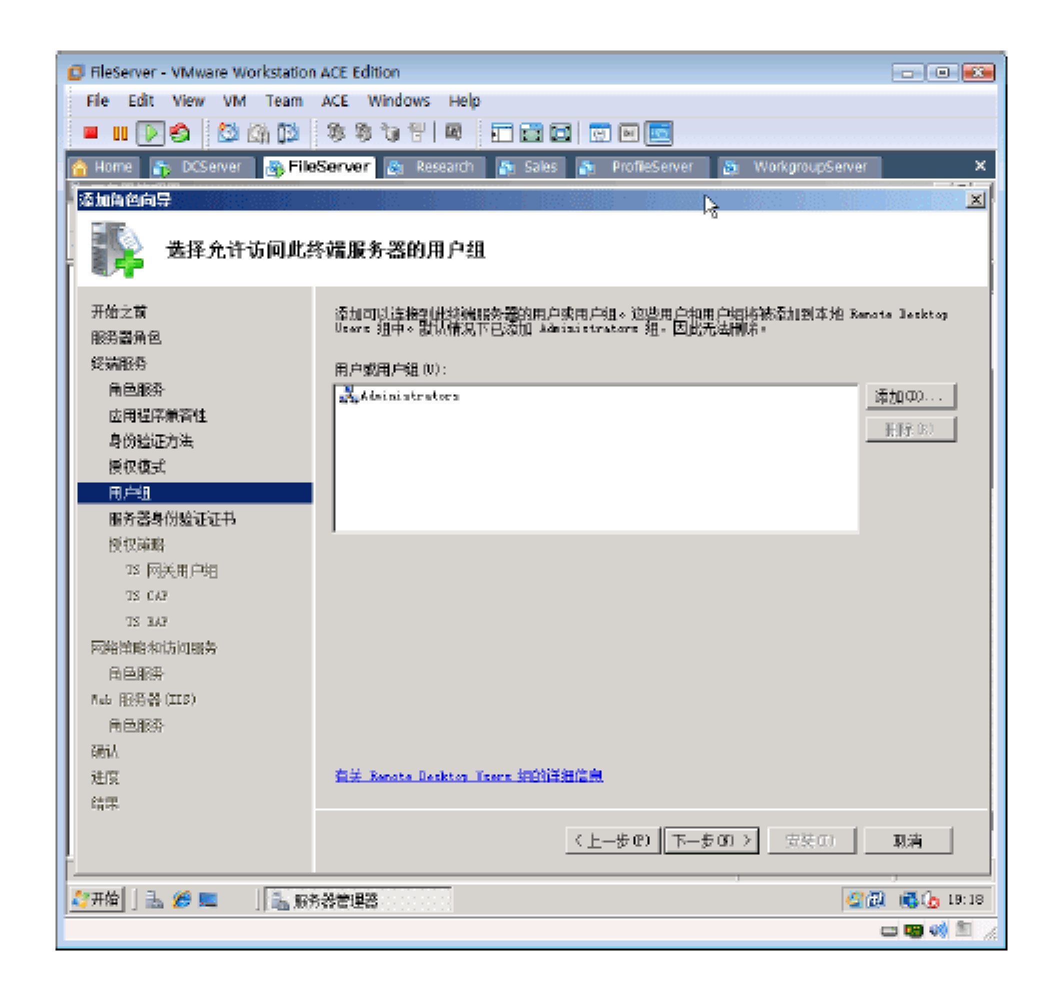


图 12-70　选择用户组

⑨ 如图 12-71 所示，在出现的“Web 服务器(IIS)”界面中，单击“下一步”按钮。

⑩ 如图 12-72 所示，在出现的“选择角色服务”界面中，单击“下一步”按钮。

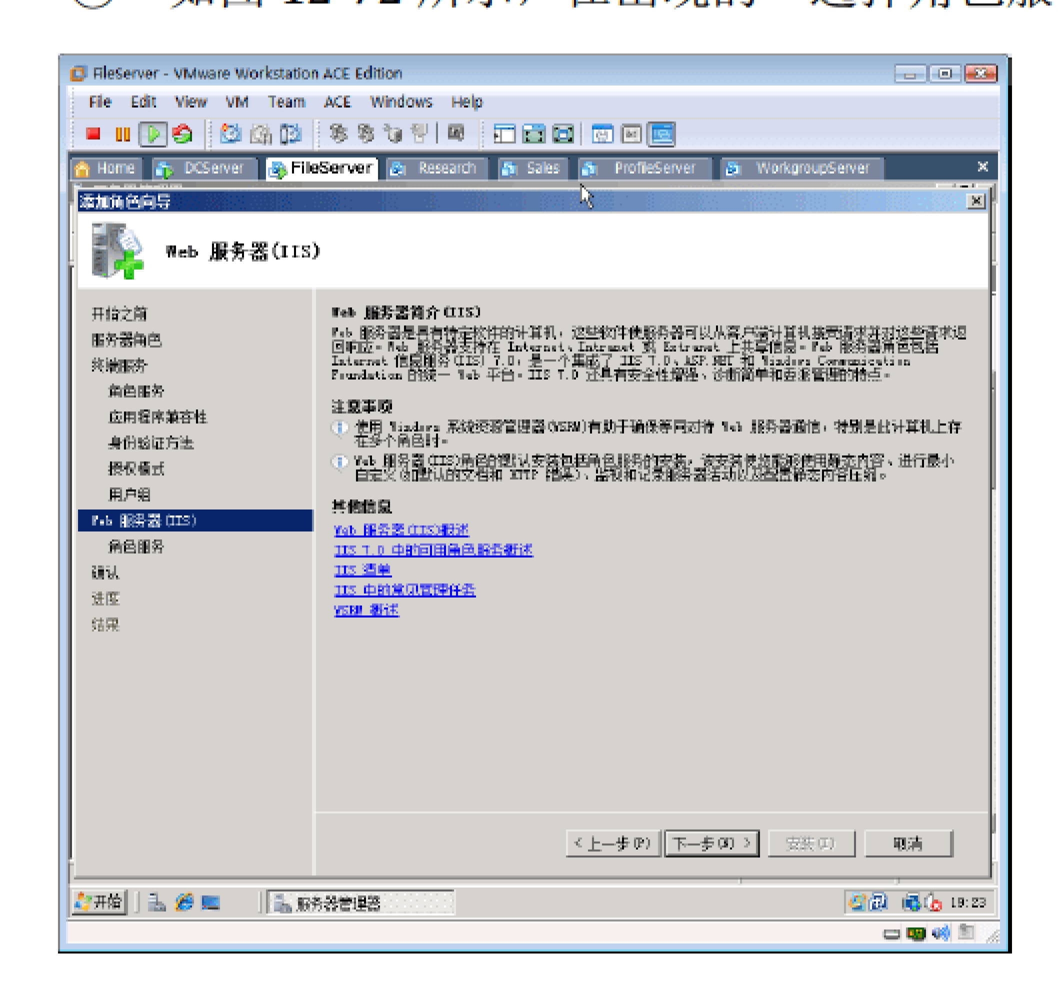


图 12-71　Web 服务器

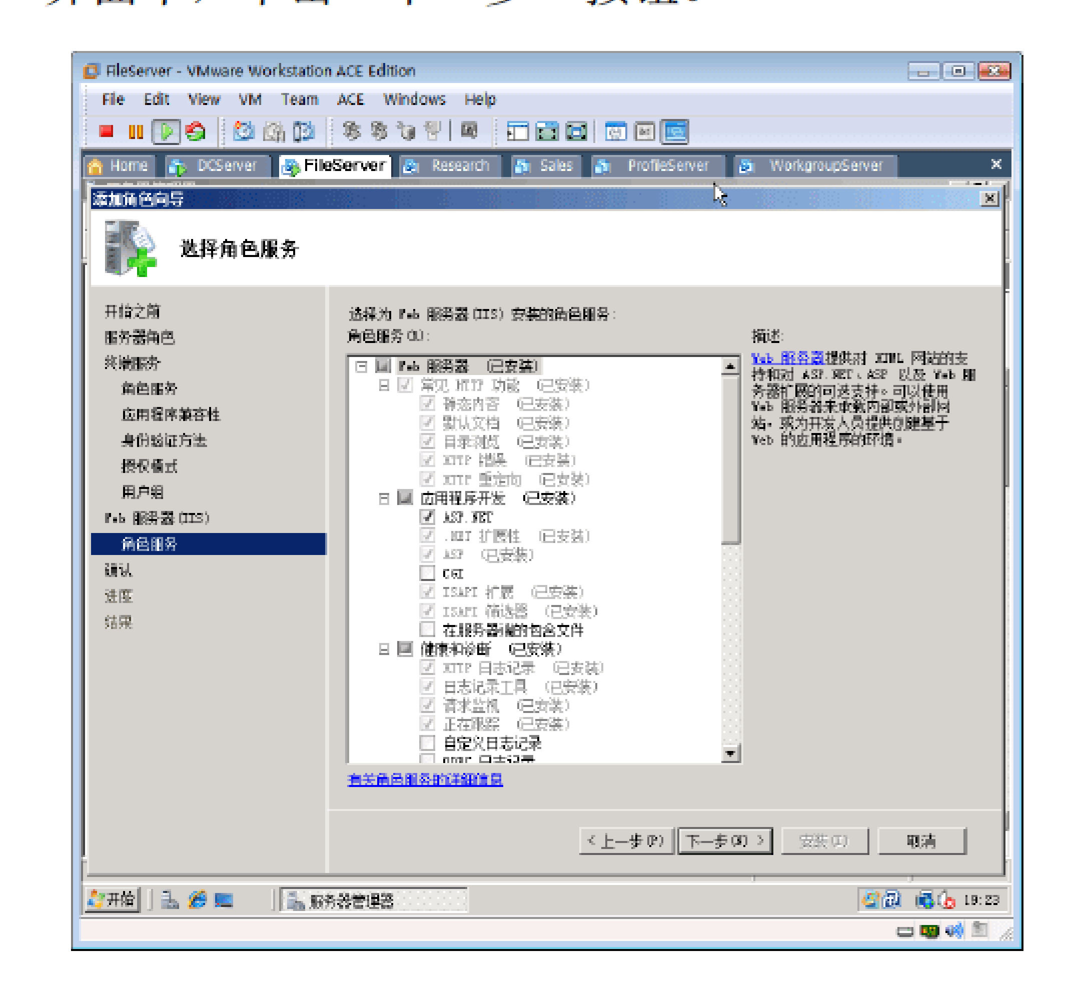


图 12-72　角色服务

⑪ 如图 12-73 所示，在出现的“确认安装选择”界面中，单击“安装”按钮。

⑫ 如图 12-74 所示，在出现的“安装结果”界面中，单击“关闭”按钮，重启系统。

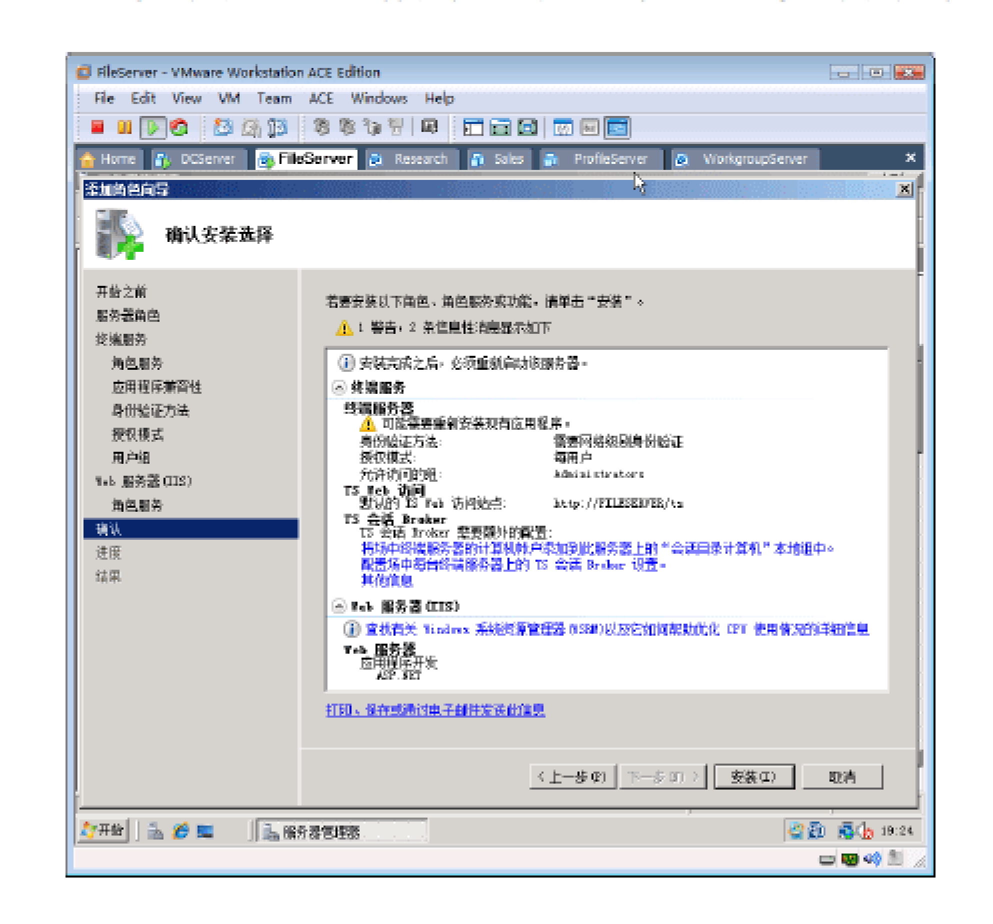


图 12-73　确认安装选择

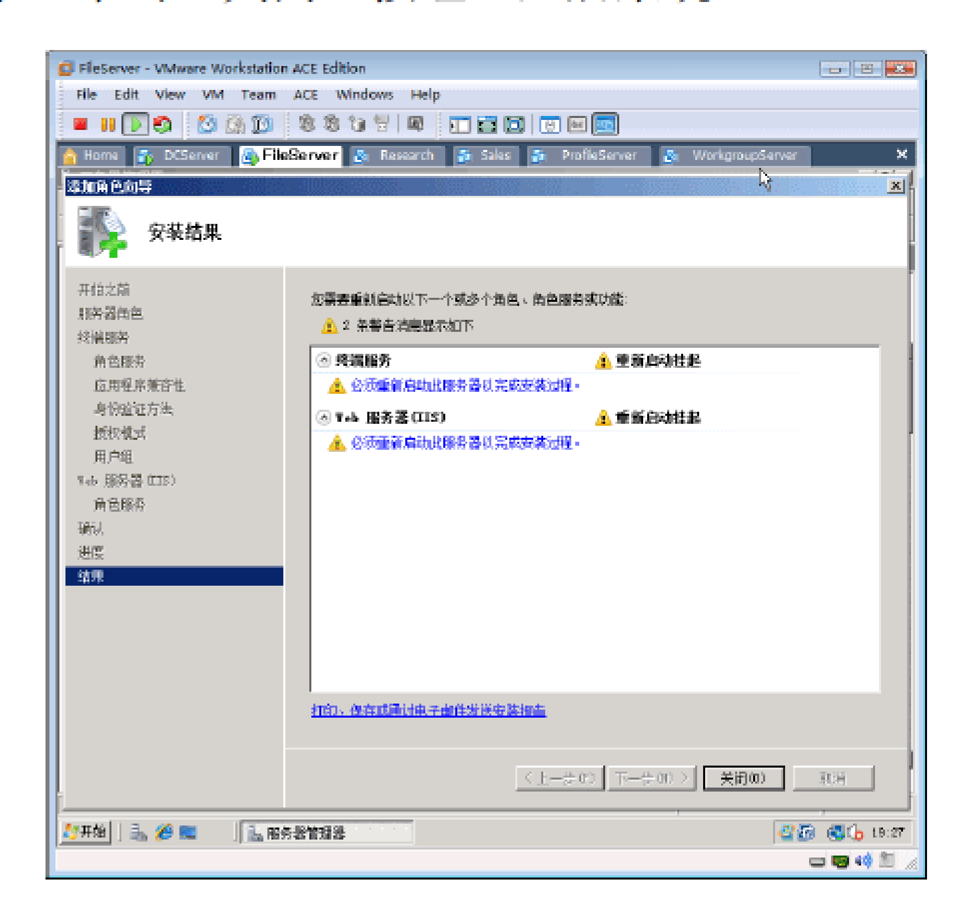


图 12-74　安装结果

12.6.4　配置终端服务器的许可证设置

指定 FileServer 使用 DCServer 终端服务授权。

① 选择“开始”→“管理工具”→“终端服务”命令，然后单击“终端服务配置”。

② 如图 12-75 所示，单击“终端服务授权模式”按钮，在出现的对话框中，选中“每用户”、“使用指定的许可证服务器”单选按钮，在文本框中输入 dcserver，单击“检查名称”按钮，提示服务器有效。

③ 单击“确定”按钮。

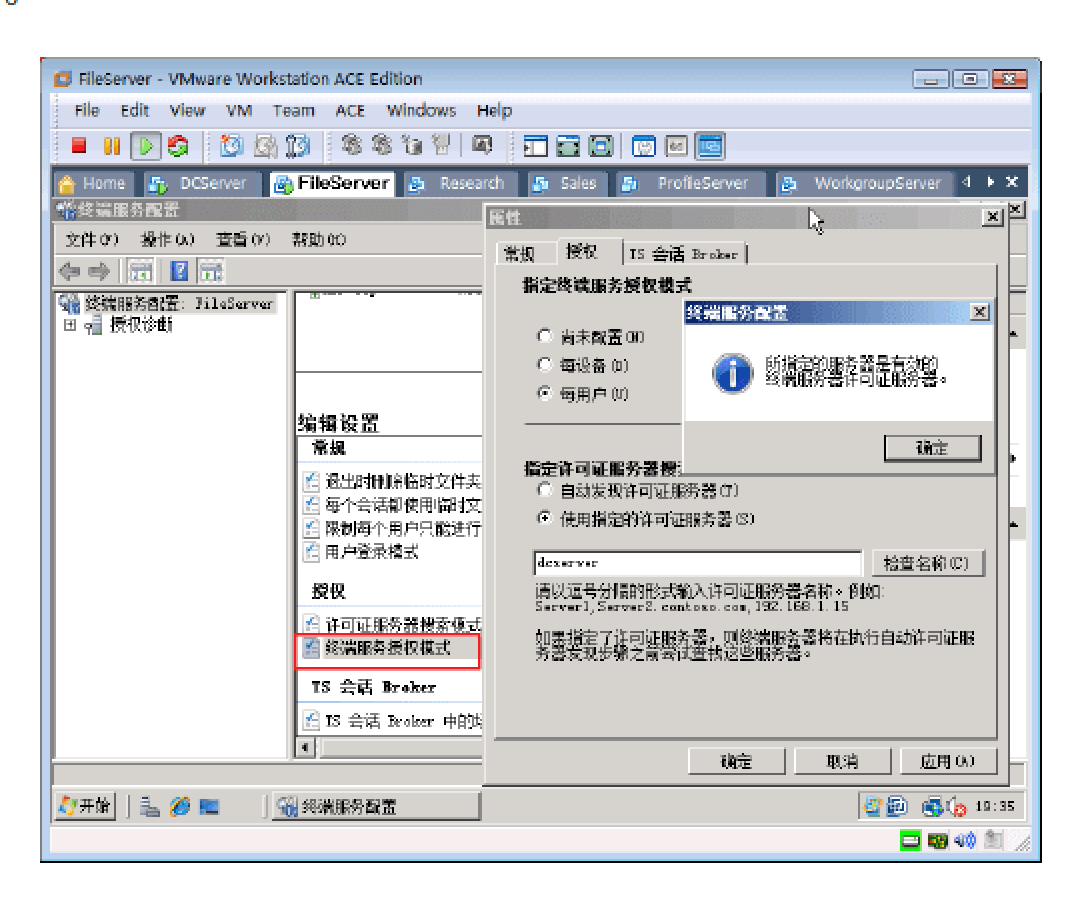


图 12-75　配置授权模式和许可证服务器

12.6.5　指定在用户登录时自动启动某个程序

为了最大化终端服务器的安全，可以指定用户连接到终端服务器时只允许特定的程序，而不是显示服

务器的桌面，防止用户对服务器进行非法操作。



注意：该功能只有在终端服务器上生效，在启用远程桌面的服务器上该设置无效。

① 选择"开始"→"管理工具"→"终端服务"命令，然后单击"终端服务配置"。

② 如图 12-76 所示，双击 RDP-Tcp，在"RDP-Tcp 属性"对话框的"环境"选项卡中，输入该服务器上程序路径和文件名，单击"确定"按钮。

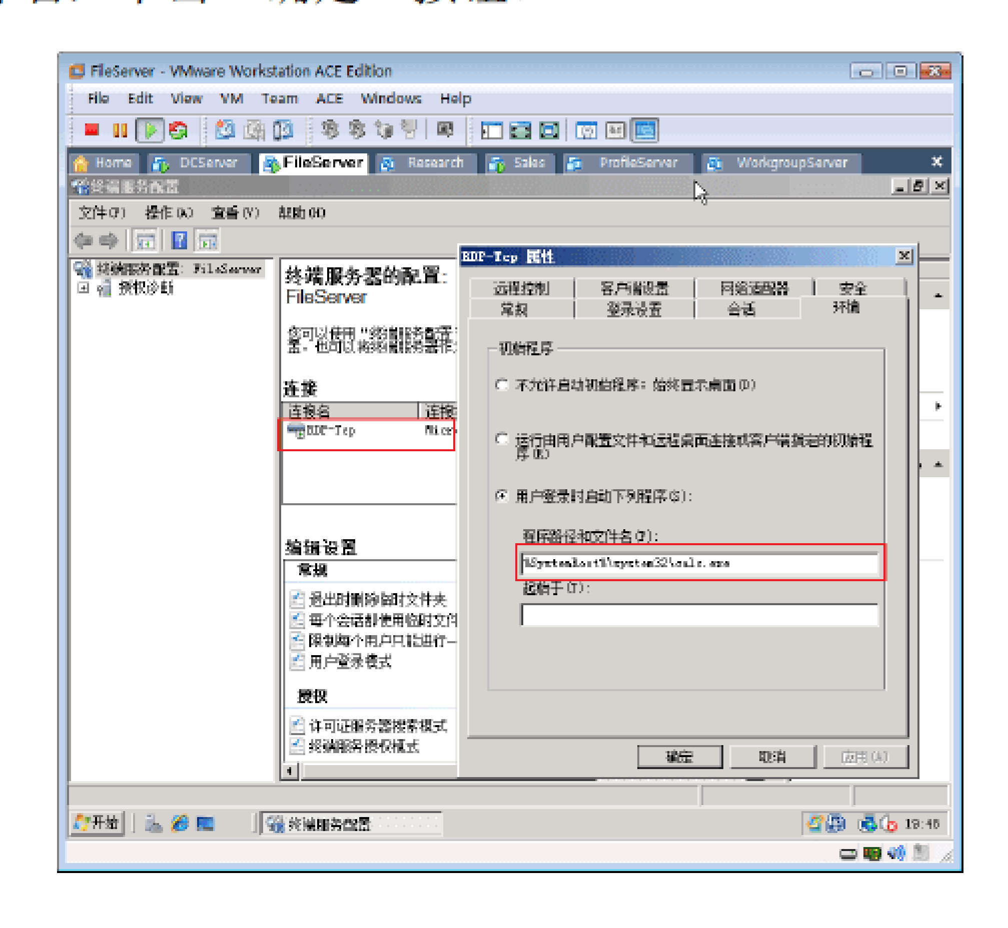


图 12-76　配置启动时启动特定程序

③ 在 Sales 计算机上测试到 FileServer 的终端服务的连接。

④ 选择"开始"→"运行"命令，在"运行"对话框中输入 mstsc，单击"确定"按钮，打开终端服务客户端。

⑤ 输入 FileServer，单击"连接"按钮，输入域管理员账户和密码。可以看到登录成功后只显示运行计算器程序，并不显示服务器桌面，如图 12-77 所示。

如果每个用户登录到终端服务器使用不同的应用程序，可以为其指定不同的应用程序。如图 12-78 所示，需要在"RDP-Tcp 属性"对话框的"环境"选项卡中，选中"运行由用户配置文件和远程桌面连接或客户端指定的初始程序"单选按钮。

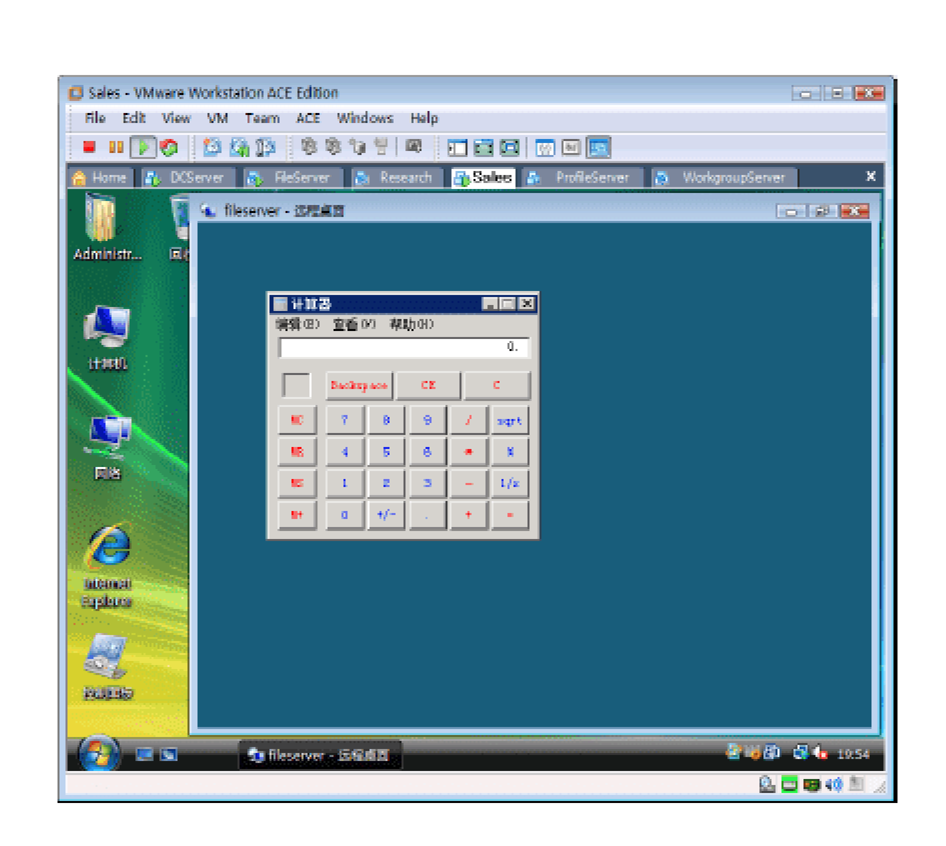


图 12-77　终端服务只启动某个程序

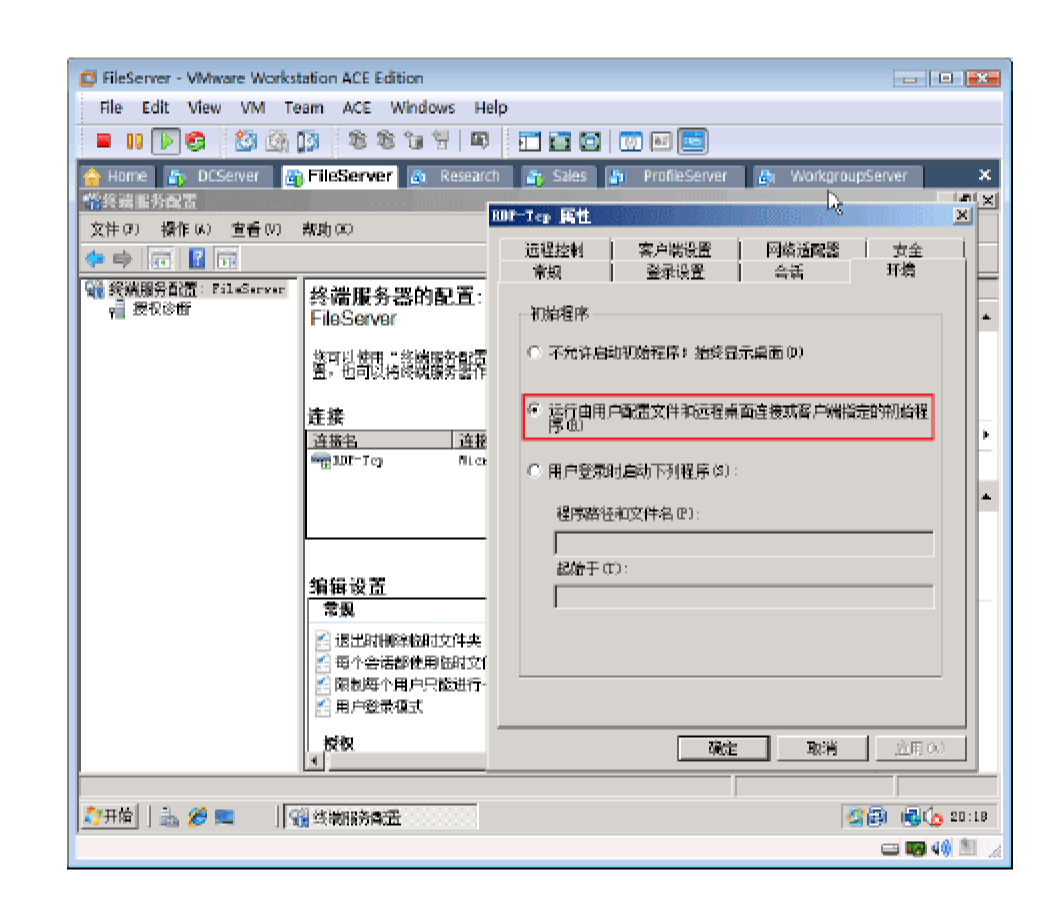


图 12-78　由用户属性确定运行的程序

⑥ 如图 12-79 所示，在用户属性的环境指定要运行的程序。

⑦ 或者在远程桌面客户端指定要运行的程序，如图 12-80 所示。

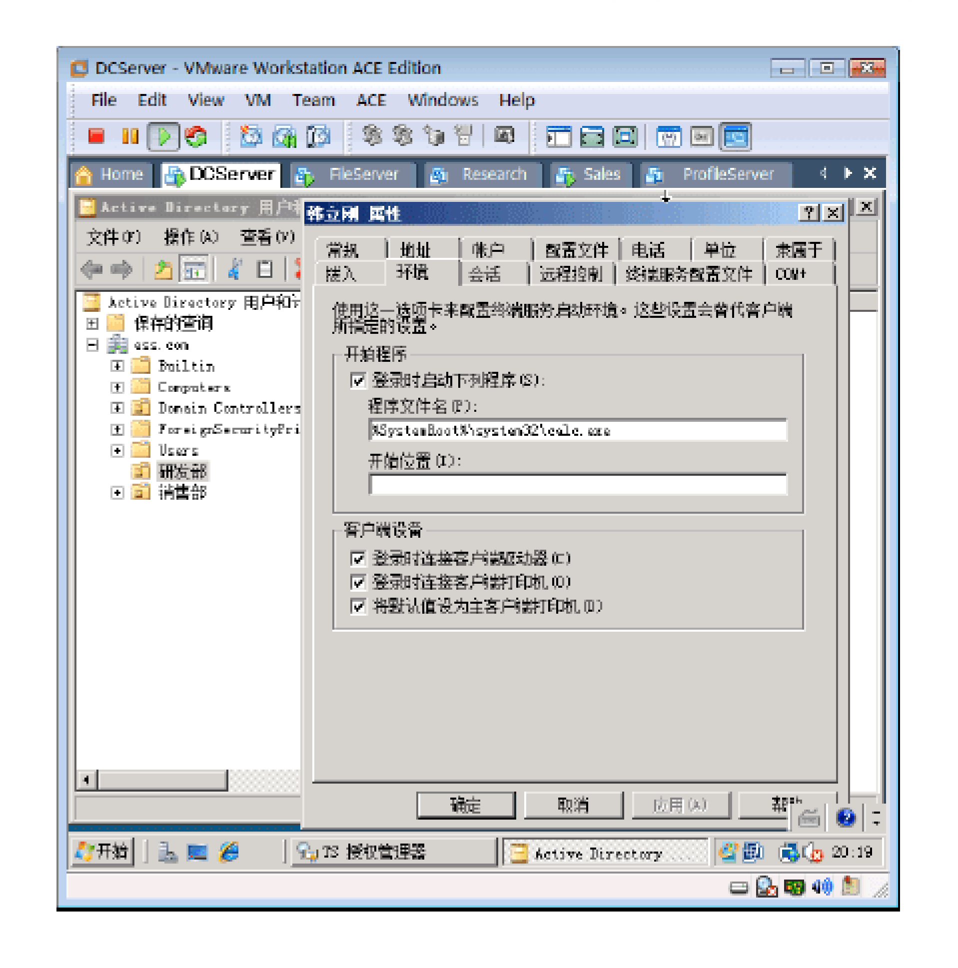


图 12-79　配置用户属性



图 12-80　在远程桌面客户端指定要运行的程序

12.6.6　查看许可证使用情况

在 DCServer 上可以查看终端服务许可证使用情况。

① 选择“开始”→“程序”→“管理工具”→“终端服务”→“TS 授权管理器”命令。

② 如图 12-81 所示，右击“报告”，在弹出的快捷菜单中选择“创建报告”→“每用户 CAL 使用情况”命令。

③ 如图 12-82 所示，在出现的对话框中，选中“整个域”单选按钮，单击“创建报告”按钮。

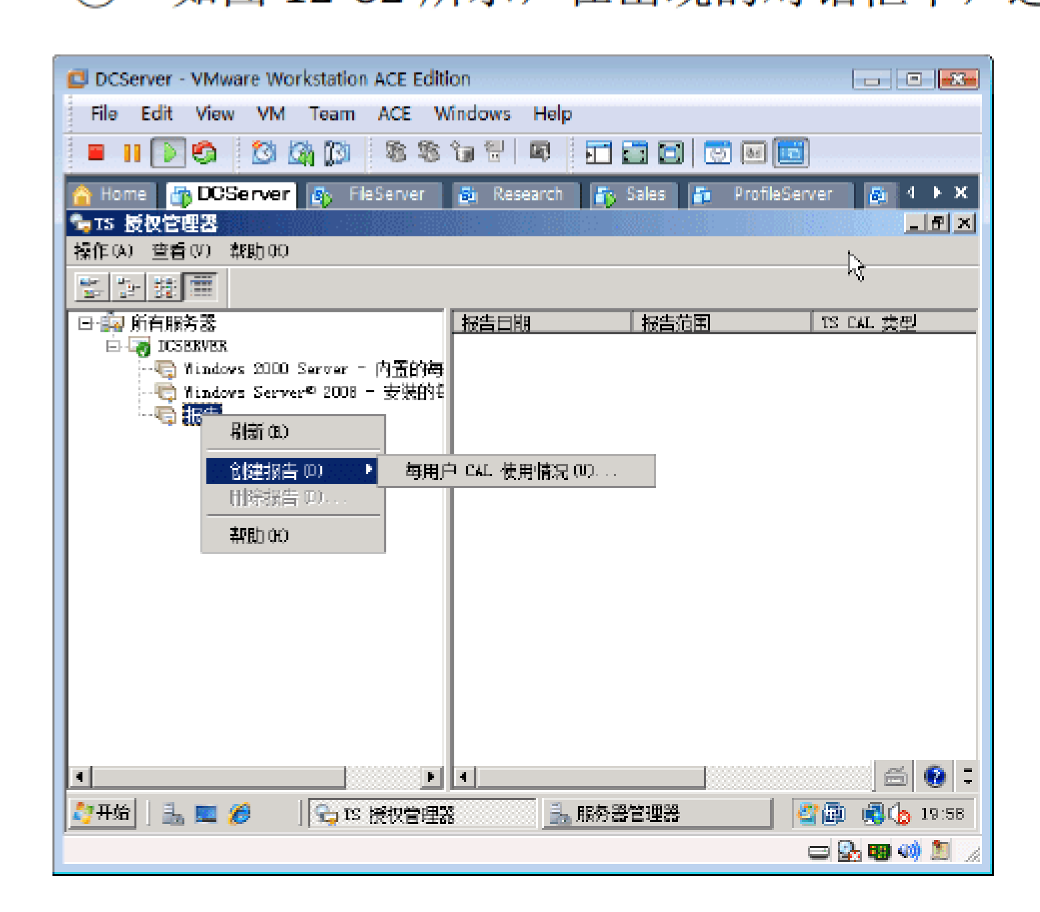


图 12-81　创建报告

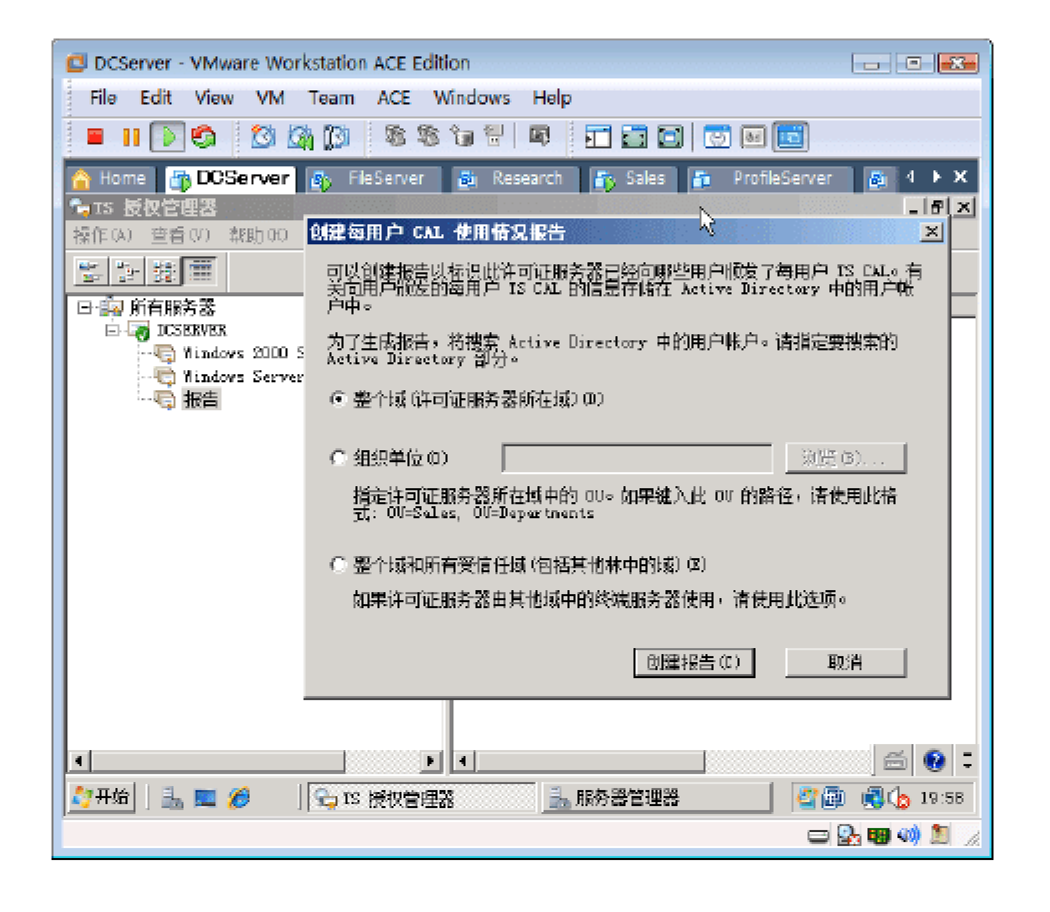


图 12-82　指定创建整个域的许可证使用报告

④ 如图 12-83 所示，可以看到 5 个 CAL，已经使用了一个。

⑤ 如图 12-84 所示，在 Sales 上使用另外一个域用户连接到 FileServer。

⑥ 如图 12-85 所示，再次在 DCServer 上生成报告。可以看到已用两个 CAL。



注意：如果使用同一个域用户连接多次 FileServer，只使用一个 CAL，因为终端服务 CAL 是每用户模式。

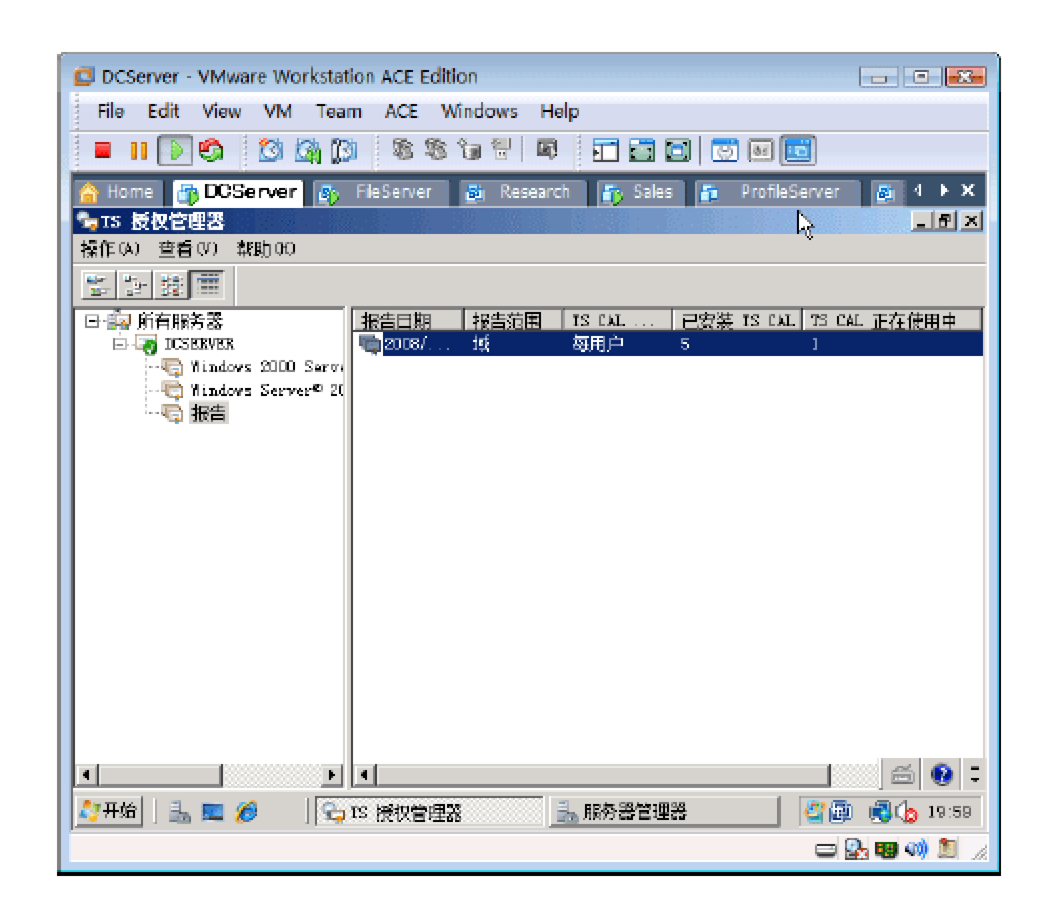



图 12-83　查看报告

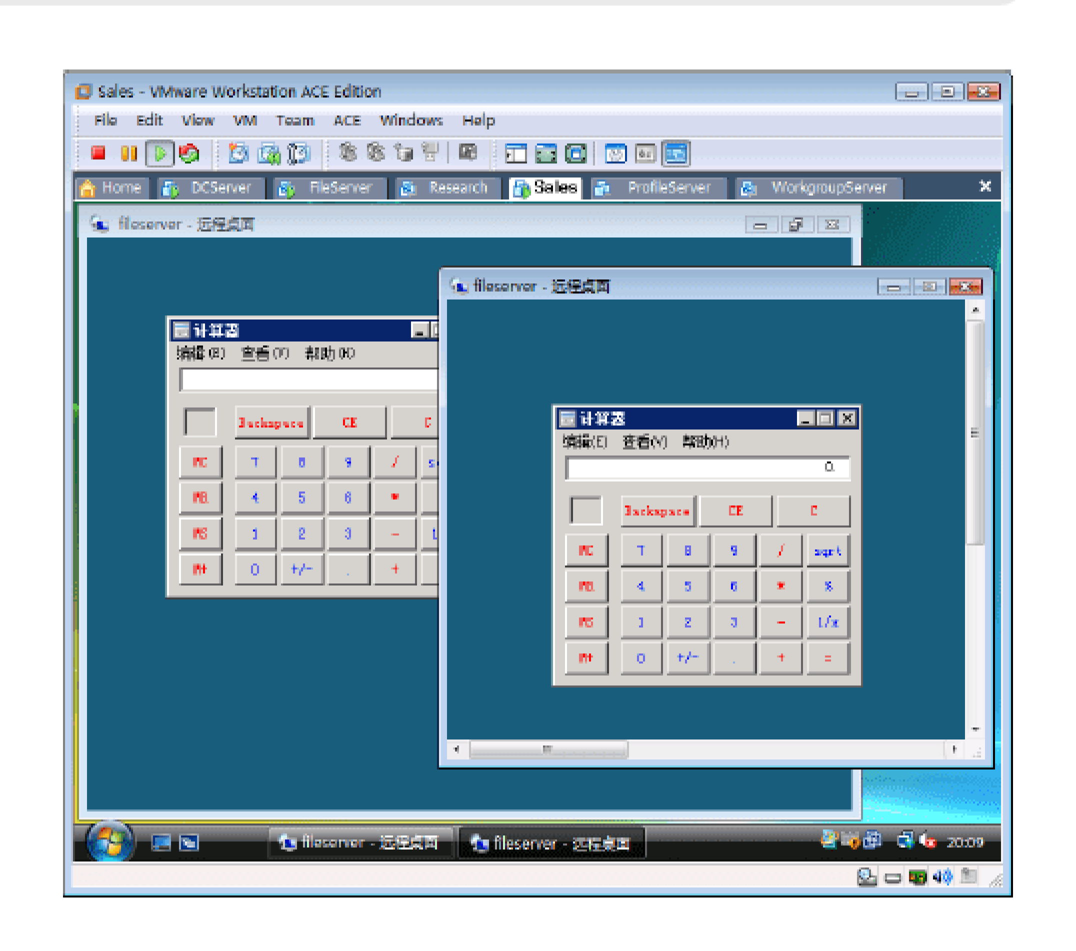


图 12-84　两个用户连接

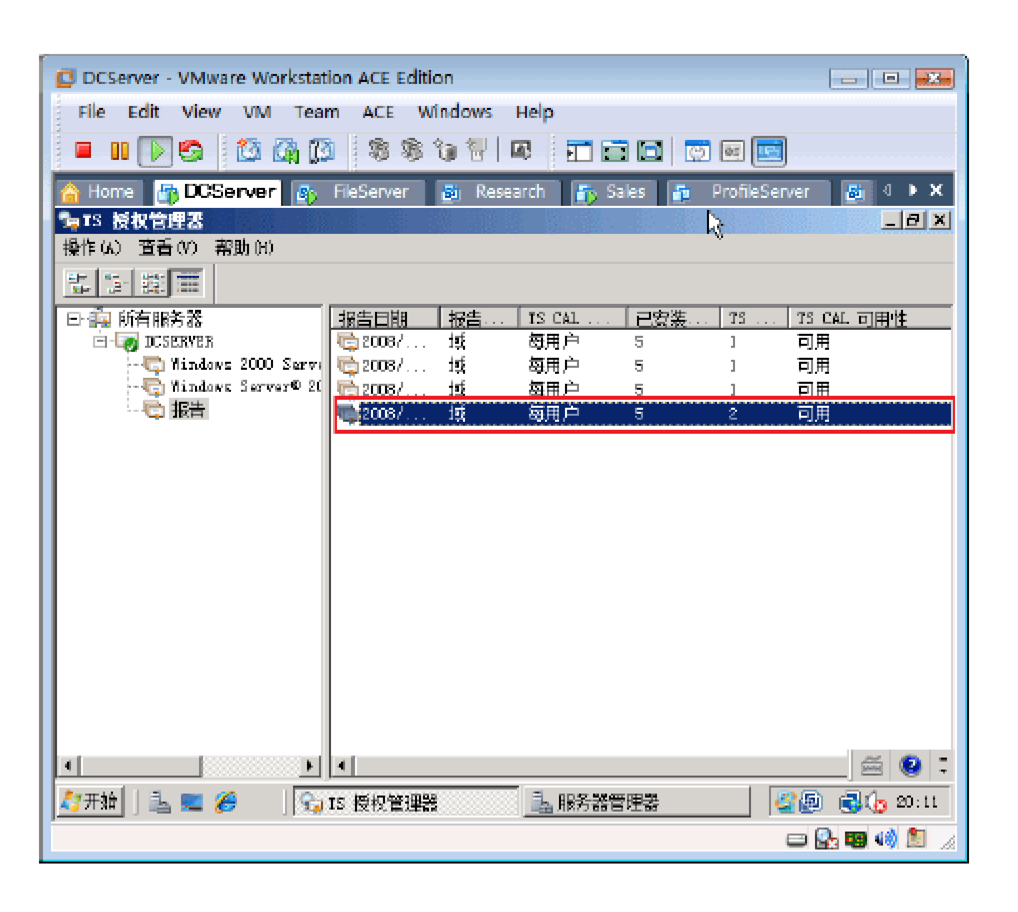


图 12-85　再次查看报告

12.7　配置和访问 RemoteApp

RemoteApp 程序是通过终端服务远程访问的程序，它们的行为就好像运行在最终用户的本地计算机上一样。用户可以将 RemoteApp 程序与本地程序并排运行。如果用户从同一台终端服务器运行多个 RemoteApp 程序，RemoteApp 程序将共享同一个终端服务会话。通过此功能可以节省用户会话，并且可以更快地连接到同一台服务器上的每个其他 RemoteApp 程序。

12.7.1　在 FileServer 上配置 RemoteApp

① 以域管理员账户登录到 FileServer，选择“开始”→“程序”→“管理工具”→“终端服务”→“TS RemoteApp 管理器”命令。

② 如图 12-86 所示，单击“添加 RemoteApp 程序”按钮。

③ 如图 12-87 所示，在出现的“RemoteApp 向导”对话框中，单击“下一步”按钮。

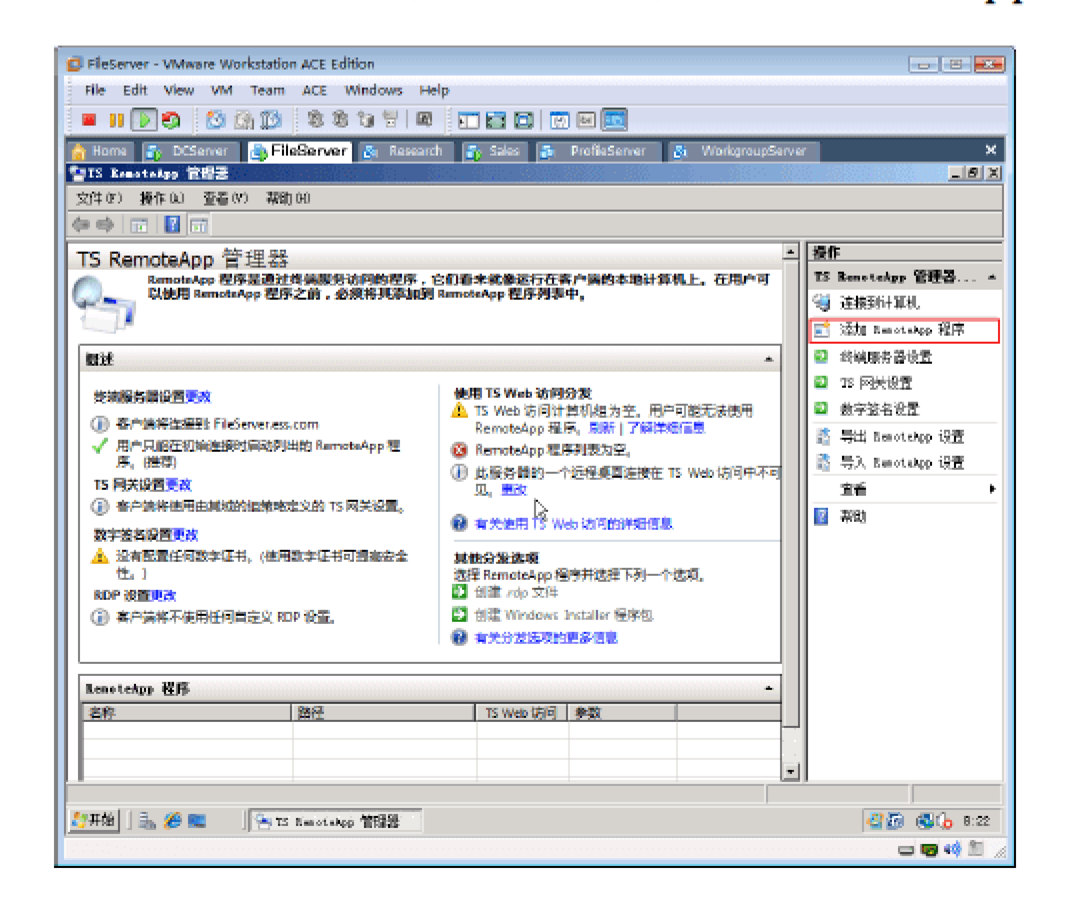


图 12-86　添加 RemoteApp

图 12-87　添加 RemoteApp 向导

④ 如图 12-88 所示，在出现的“选择要添加到 RemoteApp 程序列表的程序”界面中，选中“画图”、“计算器”和“写字板”复选框，单击“下一步”按钮。

⑤ 如图 12-89 所示，在出现的“复查设置”界面中，单击“完成”按钮。

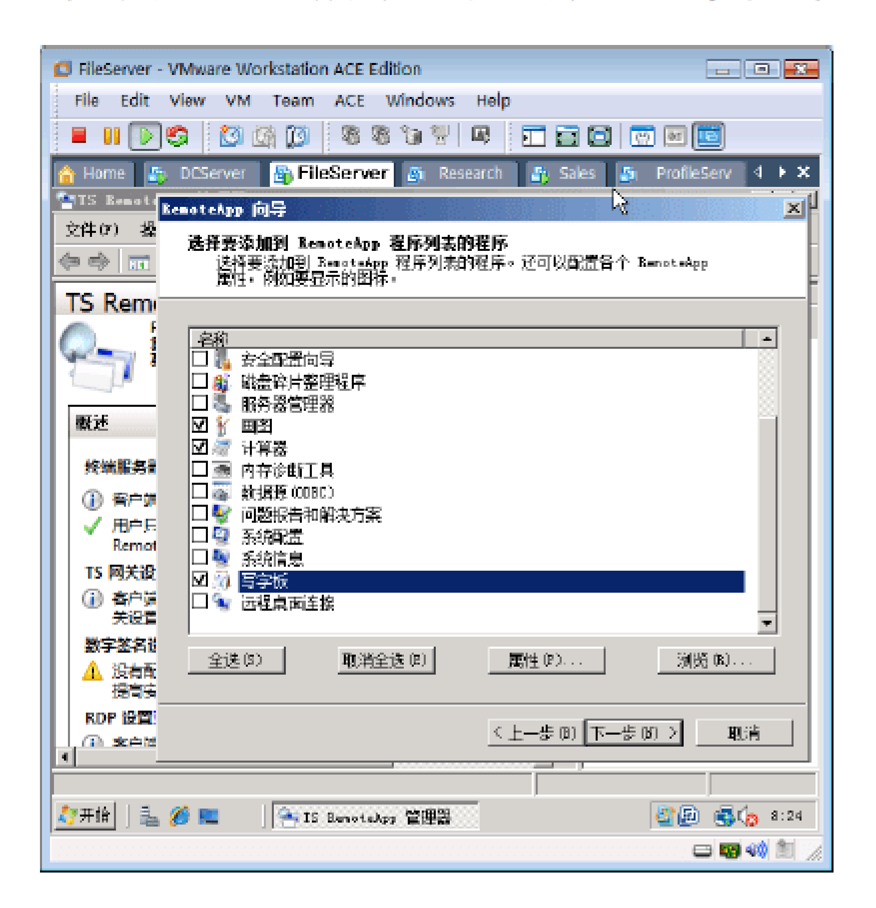


图 12-88　选择程序

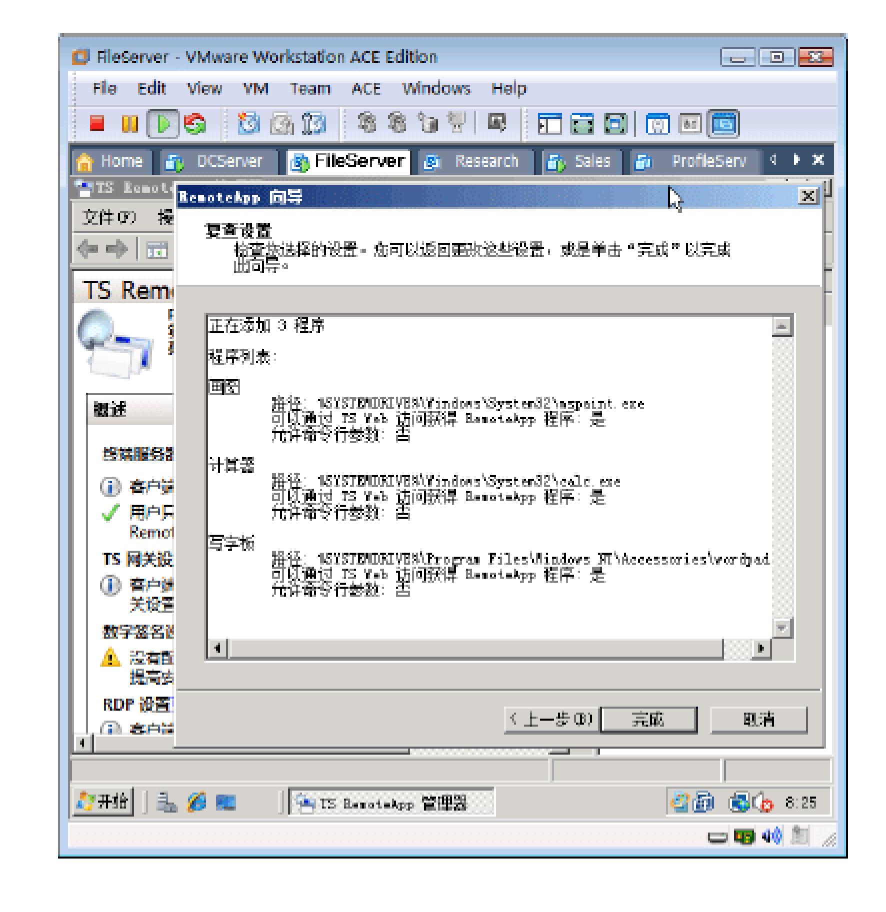


图 12-89　完成向导

⑥ 如图 12-90 所示，可以看到 RemoteApp 程序。

可以通过多种方式将 RemoteApp 程序分发给用户。根据选择的方法，用户可以进行以下操作。

- 使用 TS Web Access 在网站上访问该程序的链接。

  TS Web Access 是一项“终端服务”角色服务，使 RemoteApp 程序可由用户通过 Web 浏览器进行访问。

- 双击已由管理员创建并分发的 .rdp 文件。

  可以创建一个远程桌面协议 (.rdp) 文件，用于将 RemoteApp 程序分发给用户。可以使用现有的软件分发进程(例如 Microsoft Systems Management Server)或通过文件共享，将 .rdp 文件分发到客户端计算机。

- 双击 Windows Installer 程序包。

  在桌面或“开始”菜单中，双击由管理员使用 Windows Installer 程序包创建并分发的程序图标。

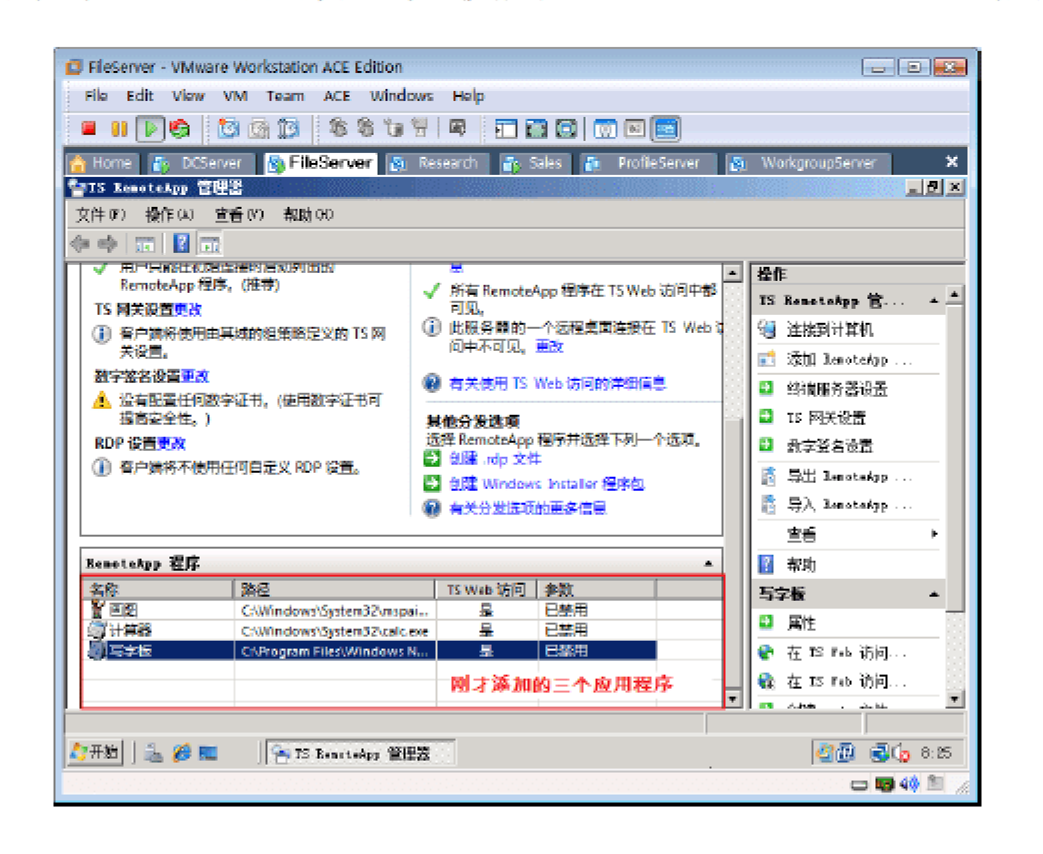


图 12-90　发布的程序

可以创建一个 Windows Installer (.msi) 程序包，用于将 RemoteApp 程序分发给用户。有关详细信息，请参阅创建 Windows Installer 程序包。若要将 Windows Installer 程序包分发到客户端计算机，可以使用现有的软件分发进程(例如 Microsoft Systems Management Server 或 Active Directory 组策略)。还可以使 Windows Installer 程序包通过文件共享进行访问。

- 双击文件扩展名与 RemoteApp 程序关联的文件。

  如果通过 Windows Installer 程序包分发 RemoteApp 程序，可以配置终端服务器是否将接管 RemoteApp 程序的客户端文件扩展名。

 **注意：***若要访问 RemoteApp 程序，客户端计算机必须至少正在运行远程桌面连接 RDC 6.0。*

12.7.2　使用 TS Web Access 在网站上访问该程序的链接

要使用 TS Web 访问终端服务器上的程序，客户端必须是以下系统之一。

- Windows Server 2008。
- Windows Vista with Service Pack 1 (SP1)。
- Windows XP with Service Pack 3 (SP3)。

① 如图 12-91 所示，在 Sales 计算机上登录，打开 IE 浏览器，输入 http://fileserver.ess.com/ts。在出现的对话框中输入用户号和密码。

② 如图 12-92 所示，右击 IE 浏览器的提示，在弹出的快捷菜单中选择“运行 ActiveX 控件”命令。在出现的“安全警告”对话框中单击“运行”按钮。

③ 如图 12-93 所示，单击网页中的“计算器”图标。

④ 如图 12-94 所示，在出现的 RemoteApp 对话框中，单击“连接”按钮。

⑤ 如图 12-95 所示，在出现的“Windows 安全”对话框中，输入用户名和密码，单击“确定”按钮。

⑥ 如图 12-96 所示，终端服务器上的计算器程序的界面出现，并没有出现远程终端服务器的桌面，这与运行本地的程序一样。

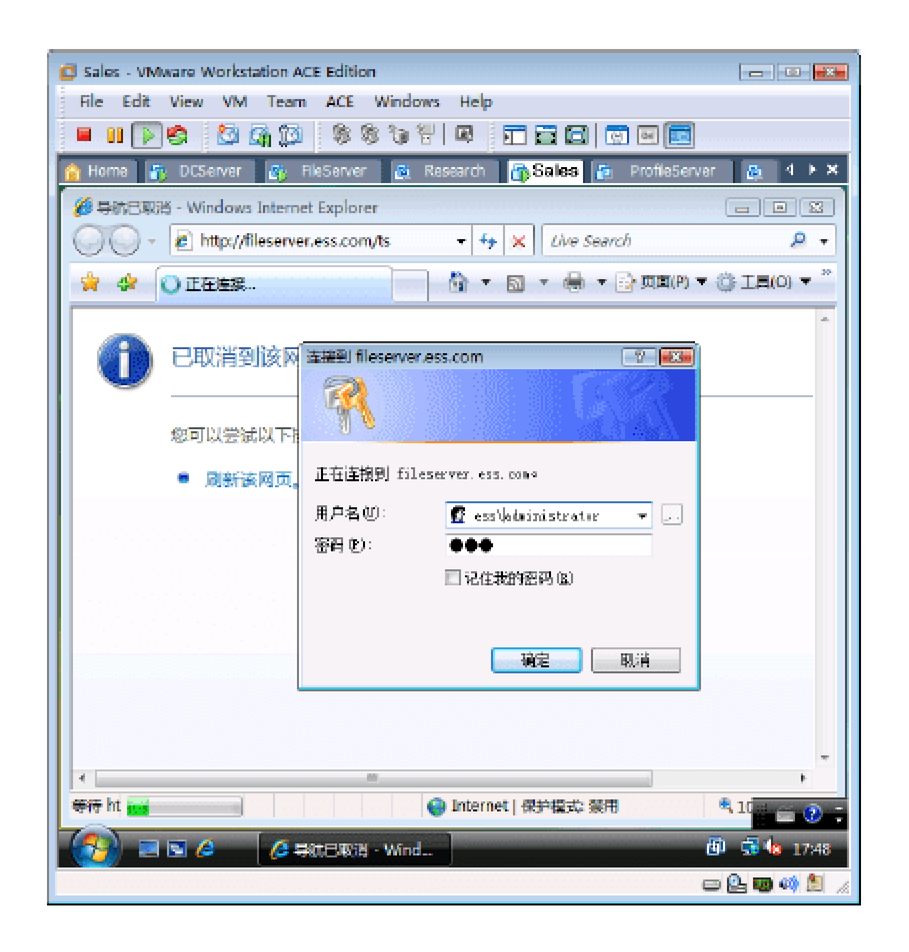


图 12-91　访问终端服务网站

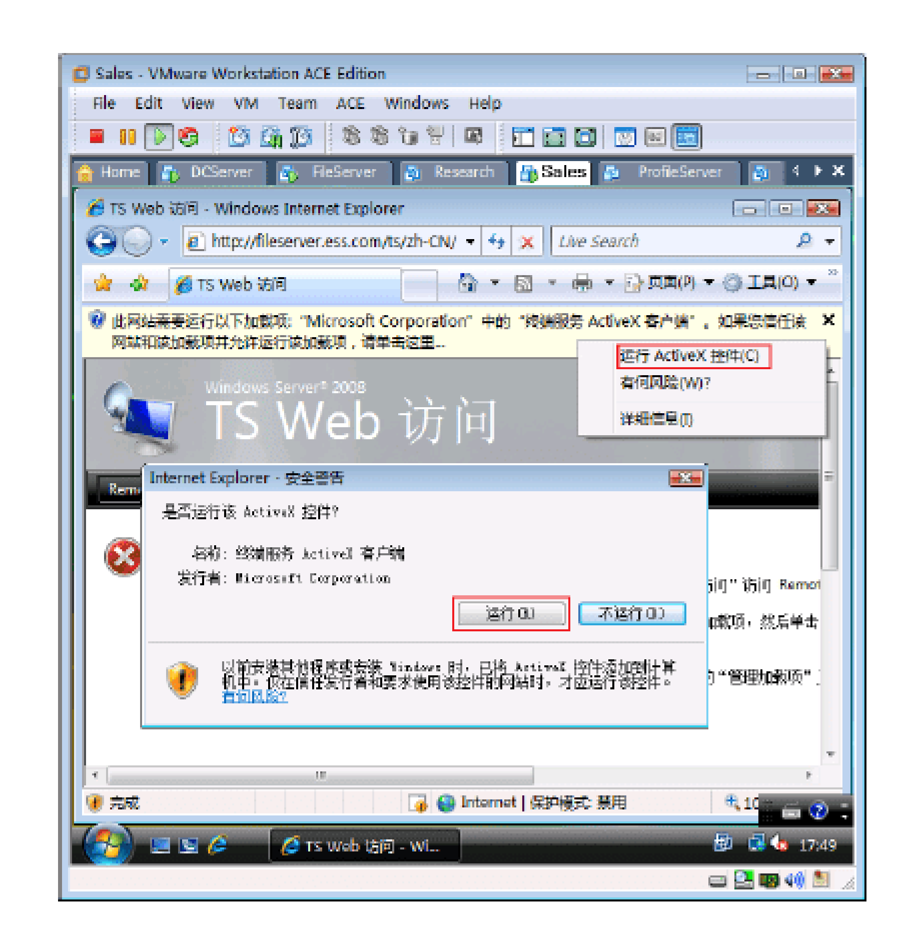


图 12-92　运行控件

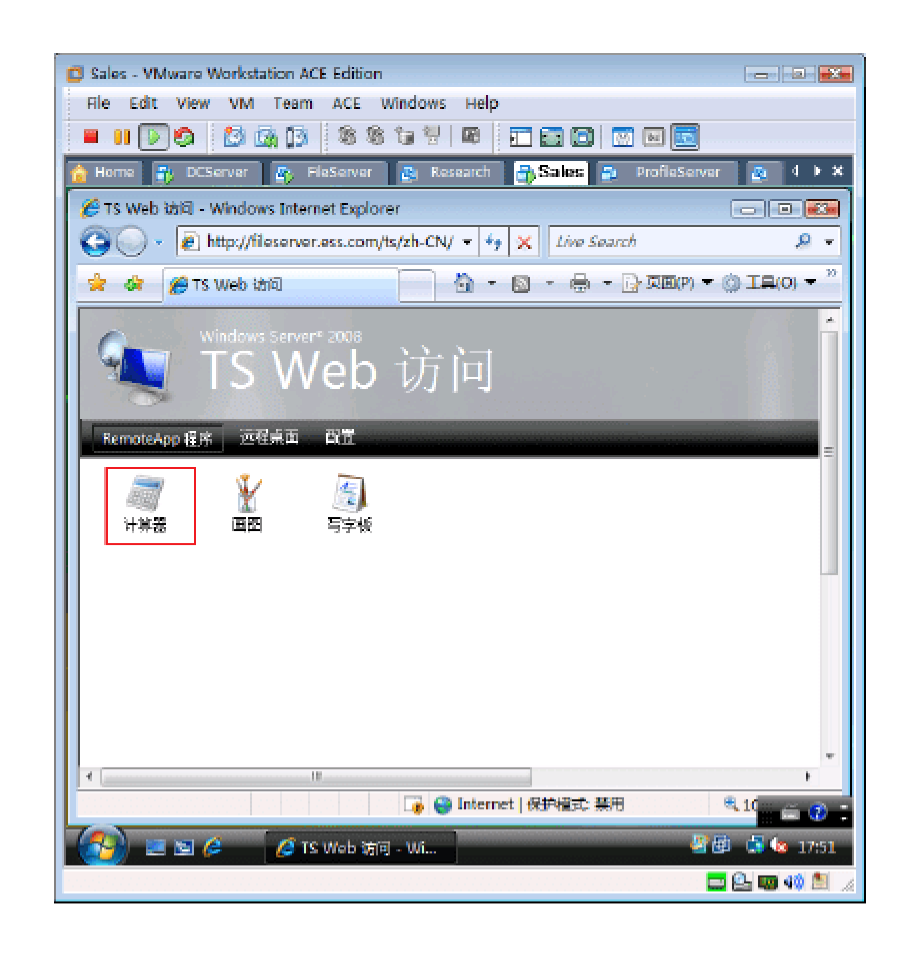


图 12-93　TS Web 访问

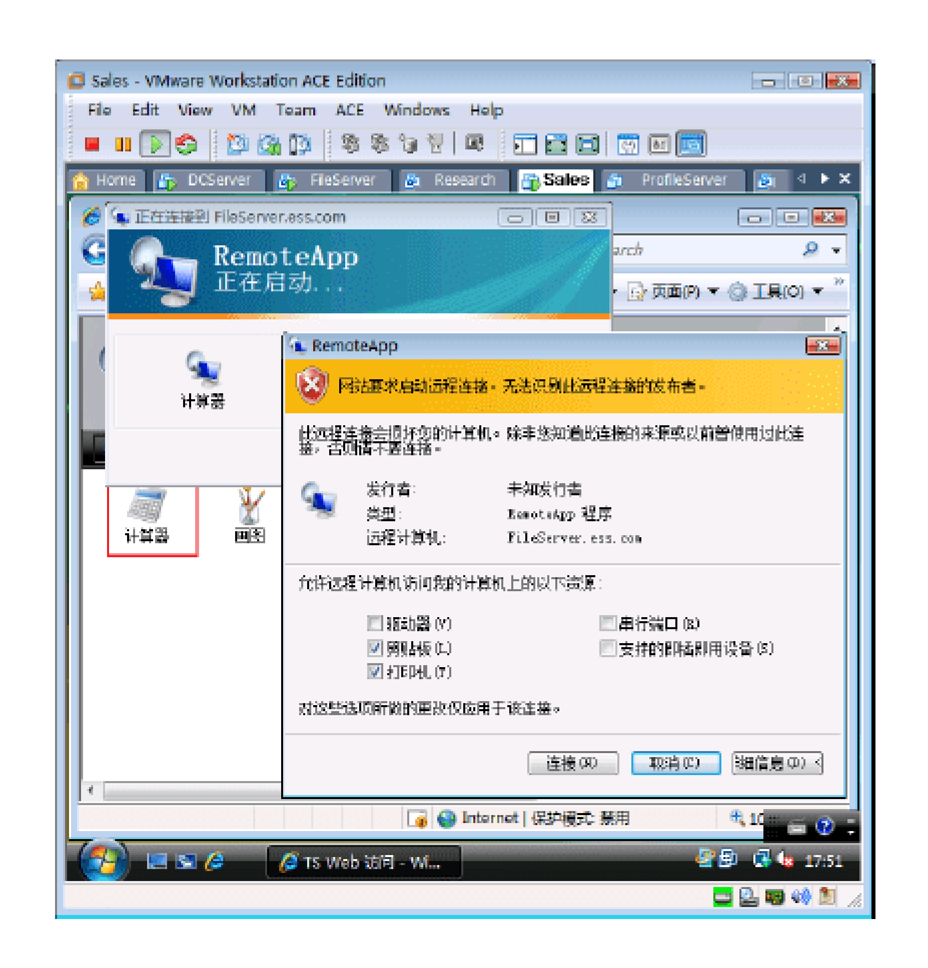


图 12-94　运行 RemoteApp

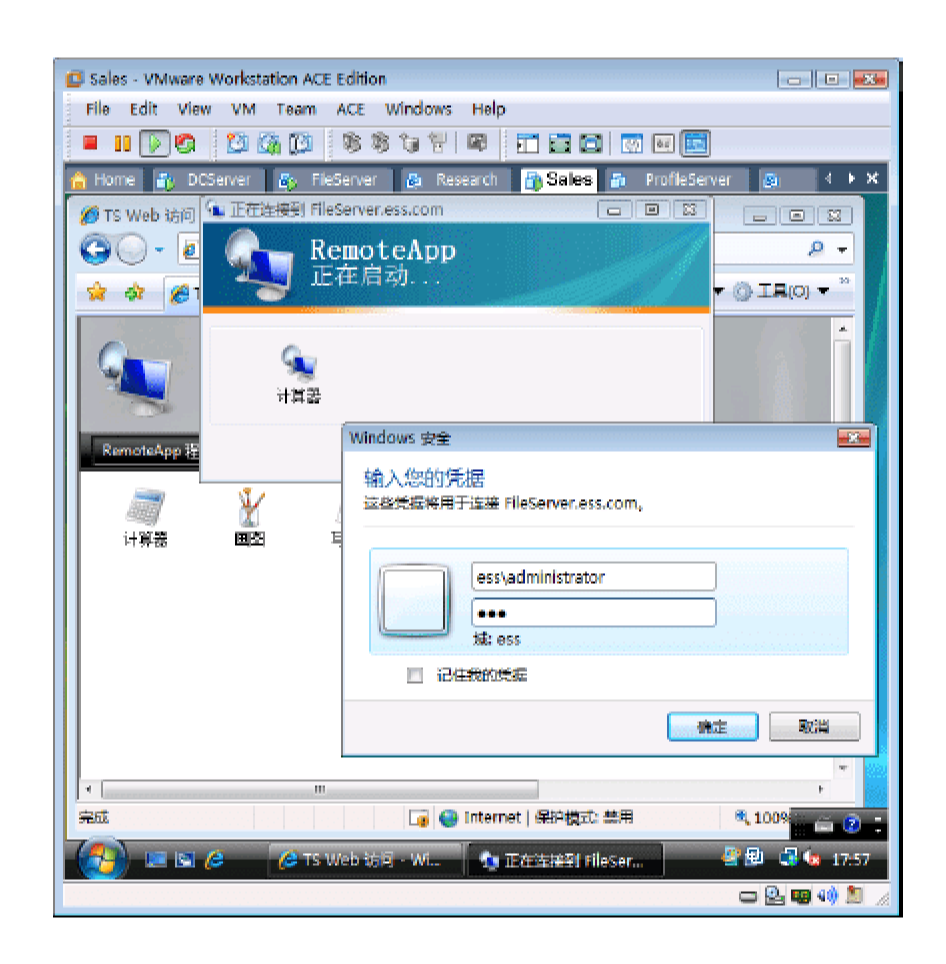


图 12-95　输入用户名和密码



图 12-96　远程应用程序演示

12.7.3　使用 rdp 文件访问 RemoteApp 上的程序

创建发布 rdp 文件使用户能够使用 RemoteApp 上的程序。

① 在 FileServer 上，选择“开始”→“程序”→“管理工具”→“终端服务”→“TS RemoteApp 管理器”命令。

② 如图 12-97 所示，选中写字板程序，单击“创建.rdp 文件”。

③ 如图 12-98 所示，在出现的向导对话框中，单击“下一步”按钮。

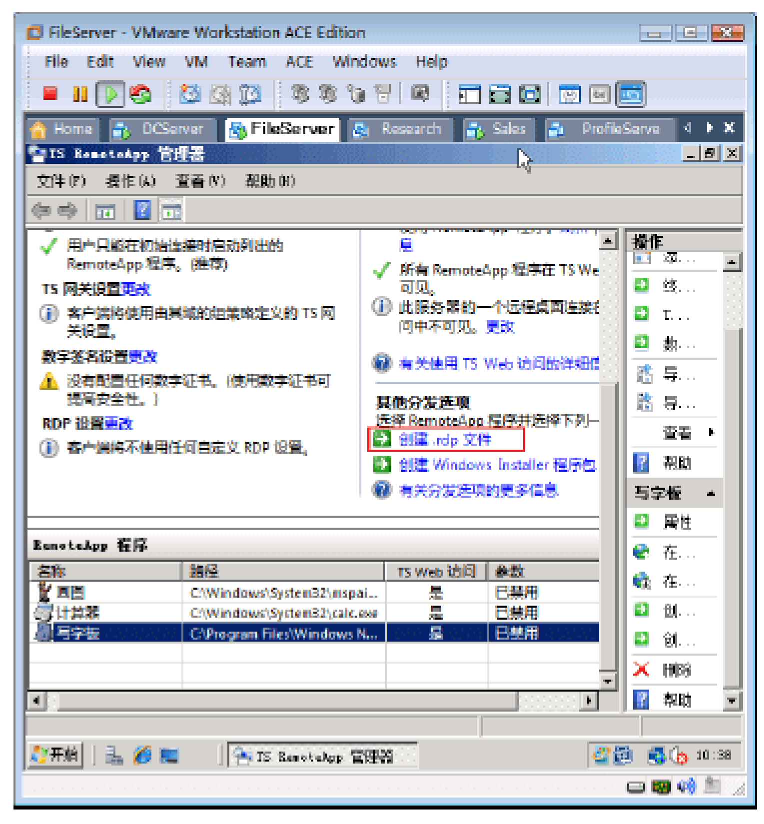


图 12-97　创建 rdp 文件

图 12-98　RemoteApp 向导

④ 如图 12-99 所示，在“指定程序包设置”界面中，输入程序包的位置，单击“下一步”按钮。

⑤ 如图 12-100 所示，在“复查设置”界面中，单击“完成”按钮。

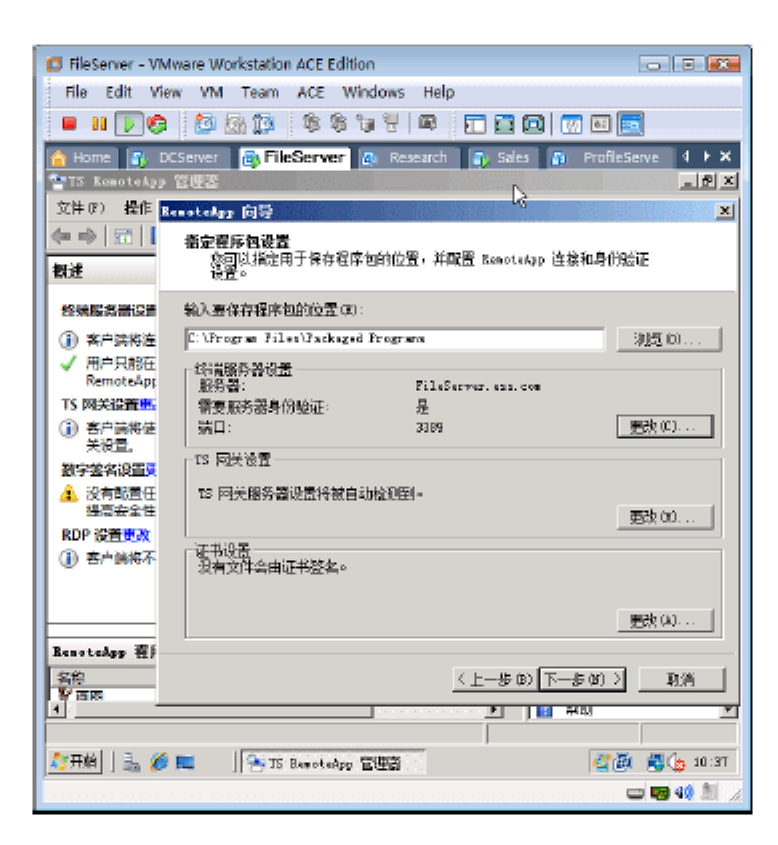


图 12-99　选择位置

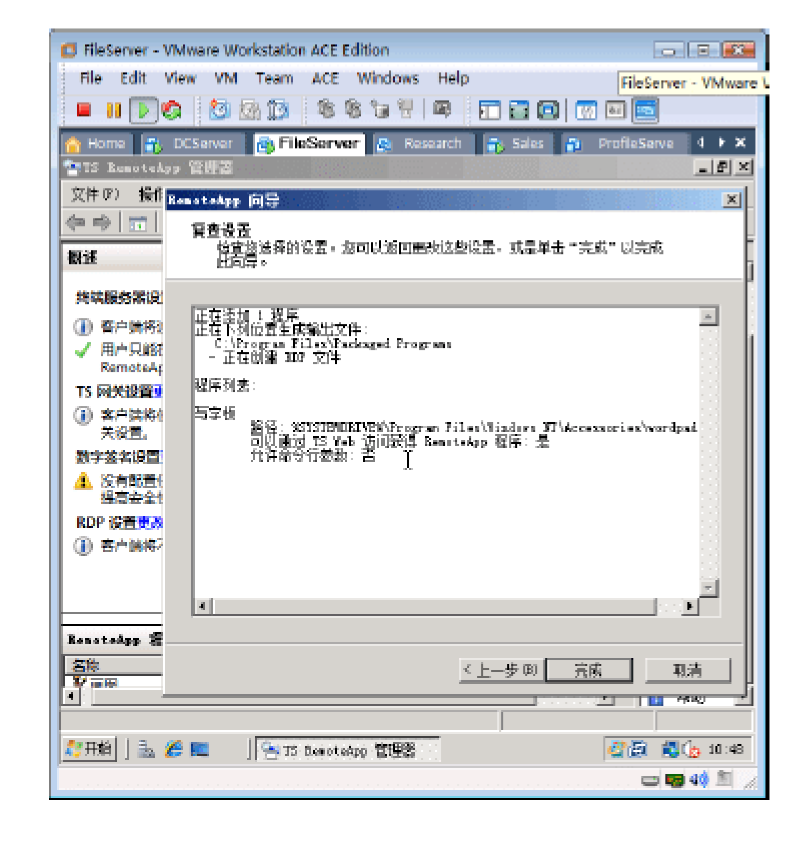


图 12-100　完成向导

⑥ 如图 12-101 所示，共享 Packaged Programs 文件夹。

⑦ 如图 12-102 所示，在 Sales 计算机将 FileServer 计算机上的 Wordpad 文件复制到桌面。

⑧ 如图 12-103 所示，双击桌面上的 Wordpad 图标，在出现的对话框中单击“连接”按钮。

⑨ 如图 12-104 所示，在“Windows 安全”对话框中，输入账号和密码，单击“确定”按钮。

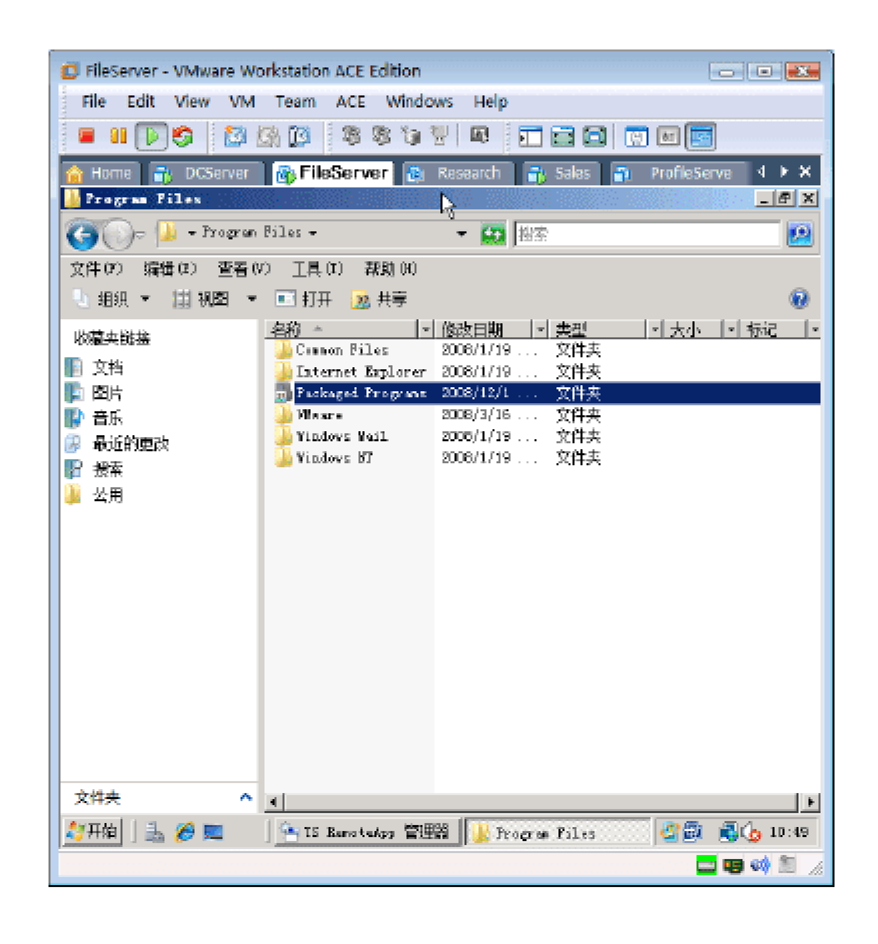


图 12-101　共享文件夹

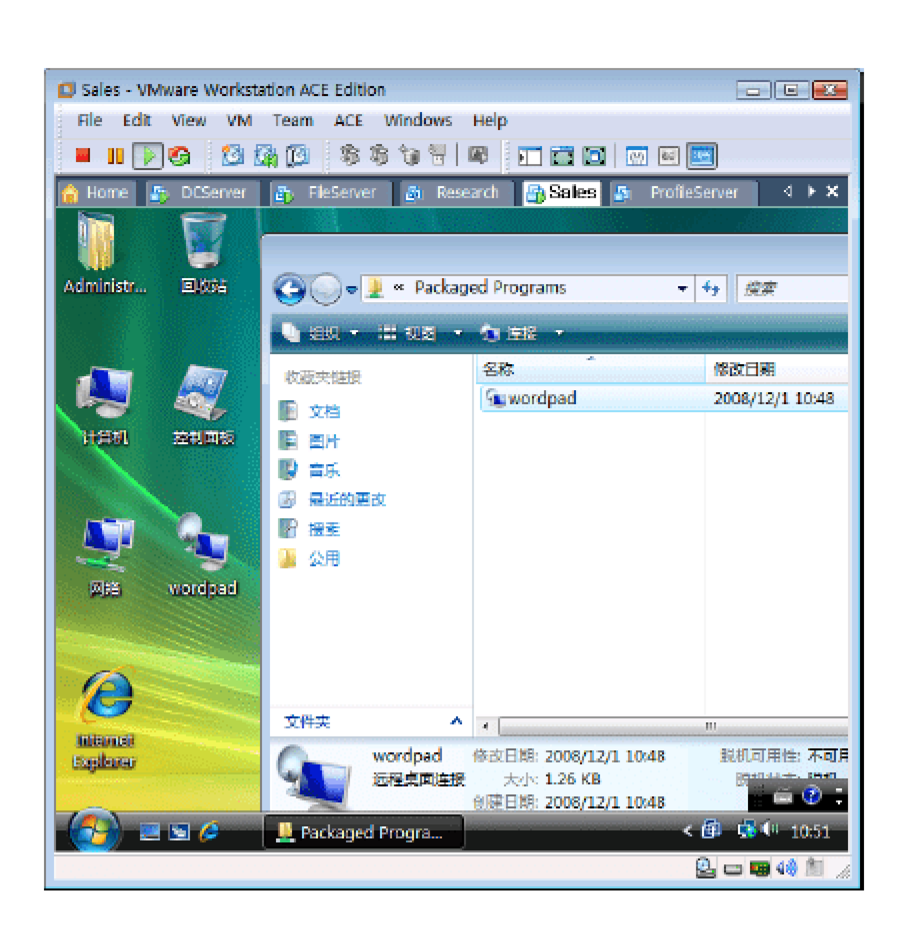


图 12-102　复制安装文件

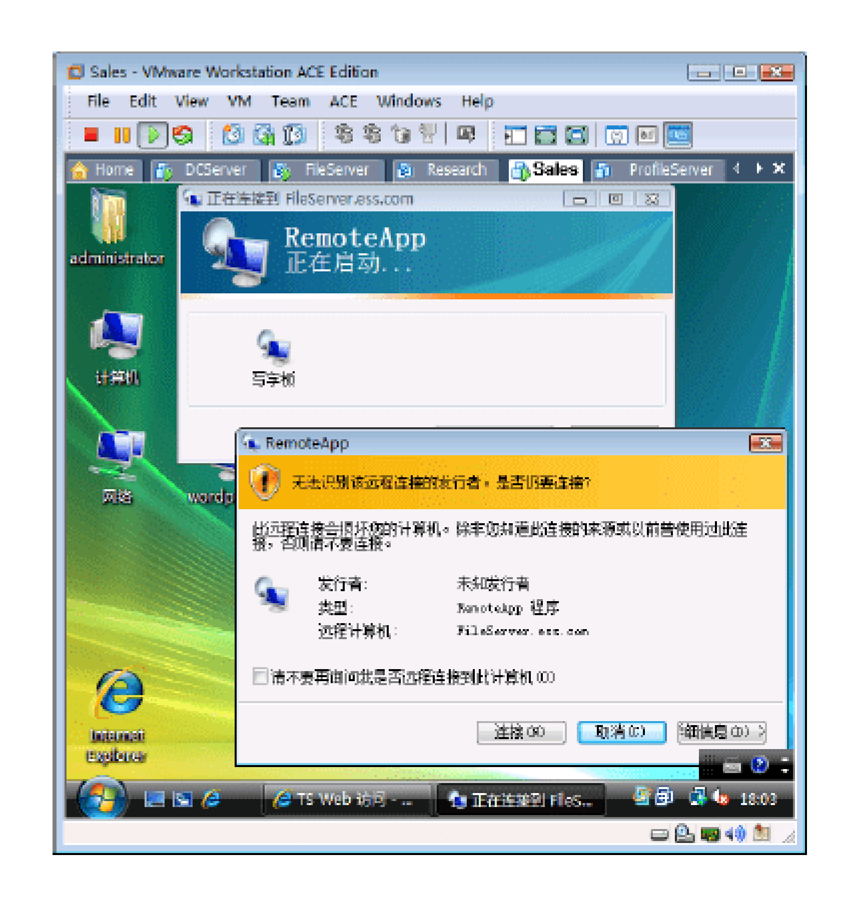


图 12-103　使用 RemoteApp

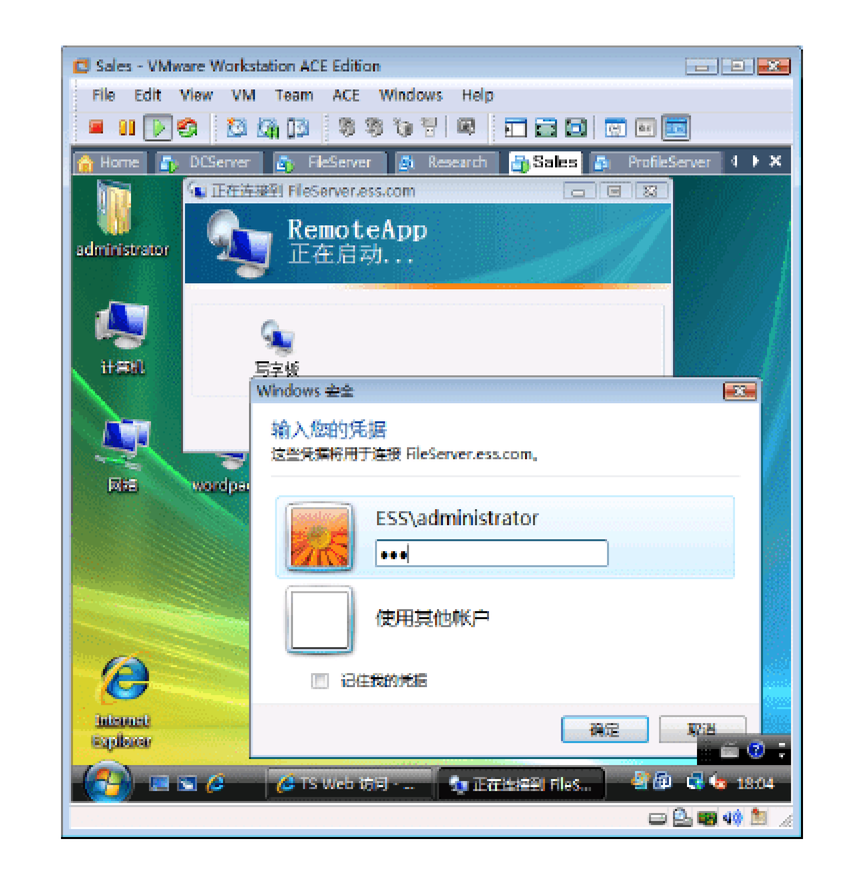


图 12-104　输入账号和密码

⑩　如图 12-105 所示，可以看到终端服务器的写字板程序已经运行。

⑪　选择写字板的“文件”→“另存为”命令，注意浏览到的是终端服务器上的目录。

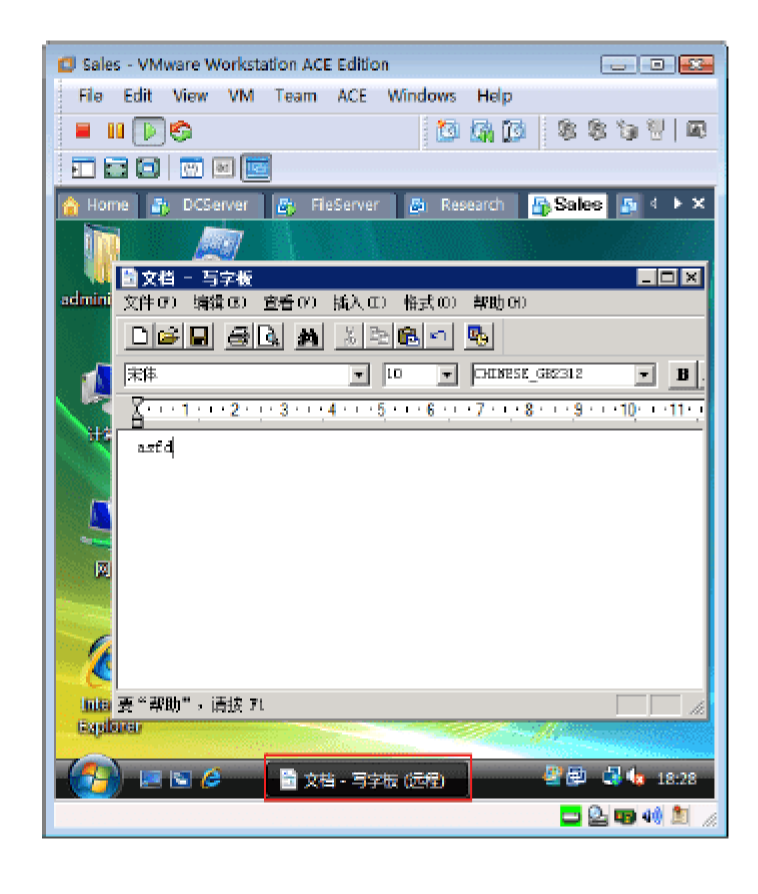


图 12-105　运行 RemoteApp

12.7.4　使用 Windows Installer 程序包部署 RemoteApp 上的程序

① 在 FileServer 上，以域管理员账户登录。

② 选择“开始”→“程序”→“管理工具”→“终端服务”→“TS RemoteApp 管理器”命令。

③ 如图 12-106 所示，选中写字板程序，单击“创建 Windows Installer 程序包”按钮。

④ 如图 12-107 所示，在出现的“RemoteApp 向导”对话框中，单击“下一步”按钮。

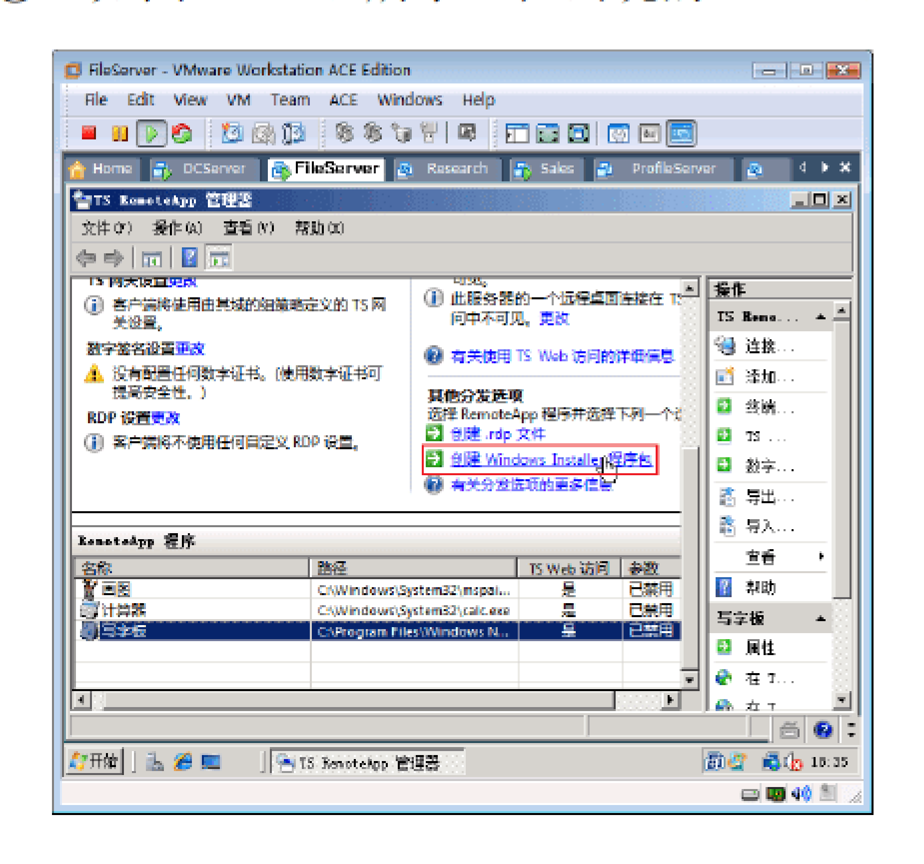


图 12-106　创建 Windows Installer 程序包

图 12-107　使用 RemoteApp 向导

⑤ 如图 12-108 所示，在“指定程序包设置”界面中，单击“下一步”按钮。

⑥ 如图 12-109 所示，在出现的“配置分发程序包”界面中，选中“桌面”复选框，在文本框中输入名称，选中“将此程序的客户端扩展与 RemoteApp 程序相关联”复选框，单击“下一步”按钮。

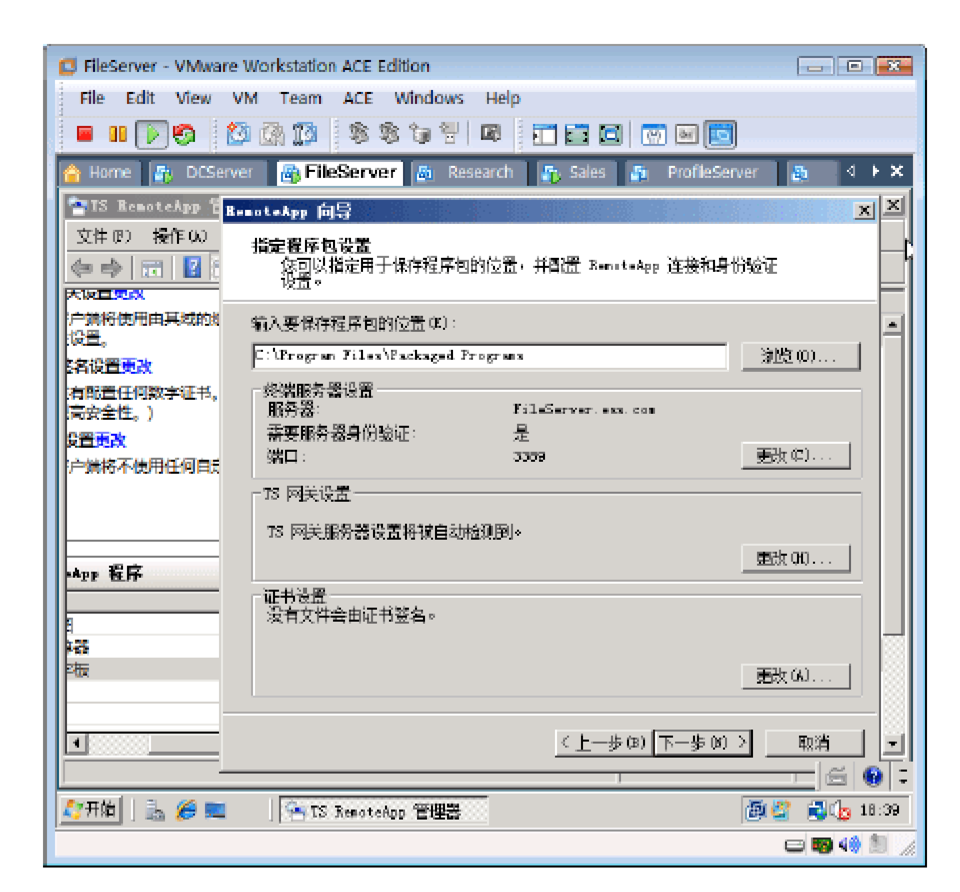


图 12-108　指定程序包位置

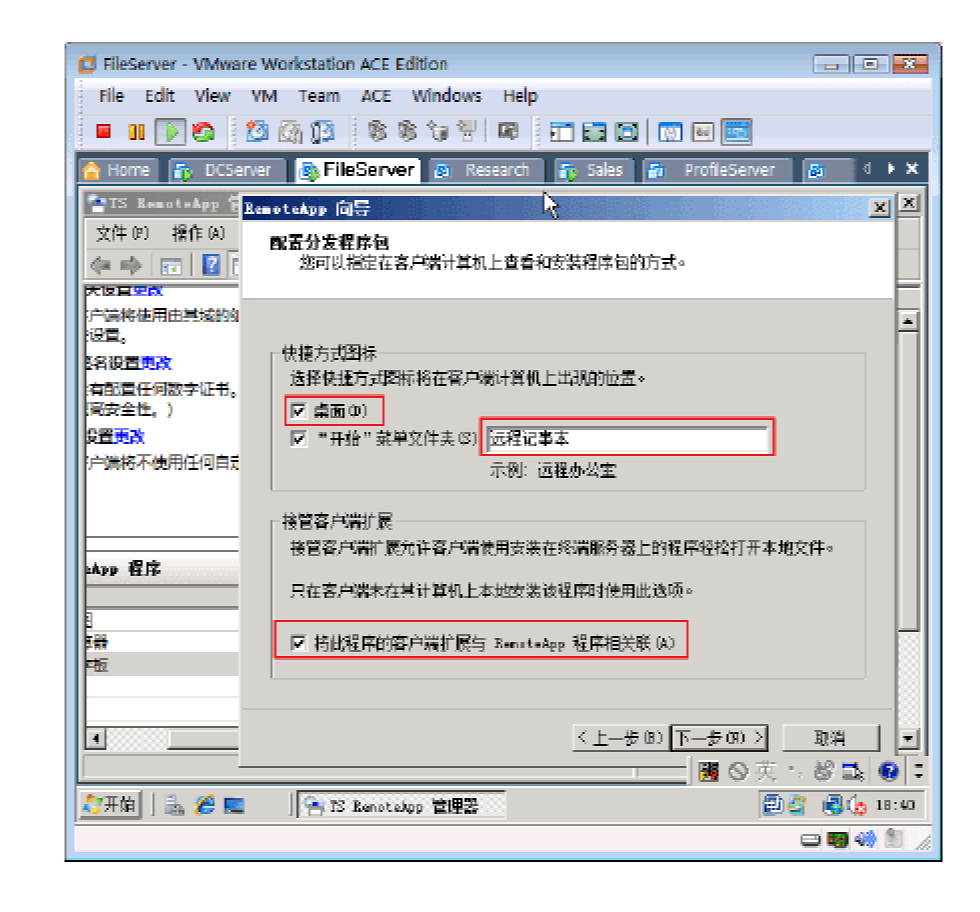


图 12-109　配置分发程序包

⑦ 如图 12-110 所示，将 FileServer 上的 wordpad.msi 安装文件复制到 Sales 的桌面，双击安装，可以看到在桌面上出现写字板的快捷方式。选择“开始”→“程序”→“远程记事本”命令，可以看到出现了“写字板”。

⑧ 如图 12-111 所示，双击桌面上的写字板快捷方式，单击“连接”按钮，输入账号和密码，可以打开远程应用程序。

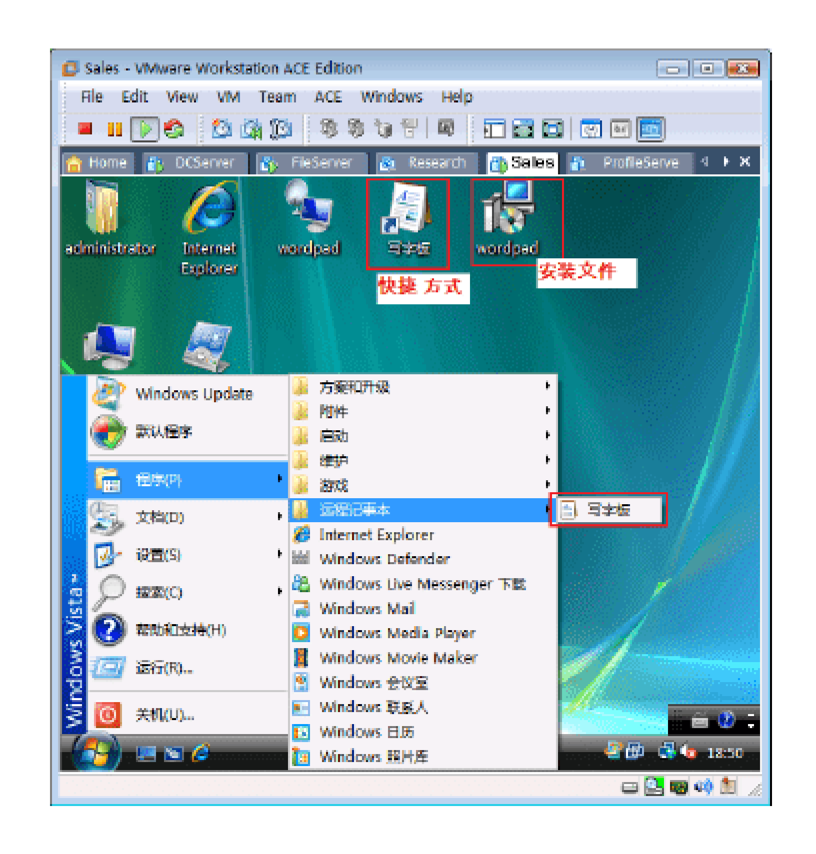


图 12-110　安装的 RemoteApp

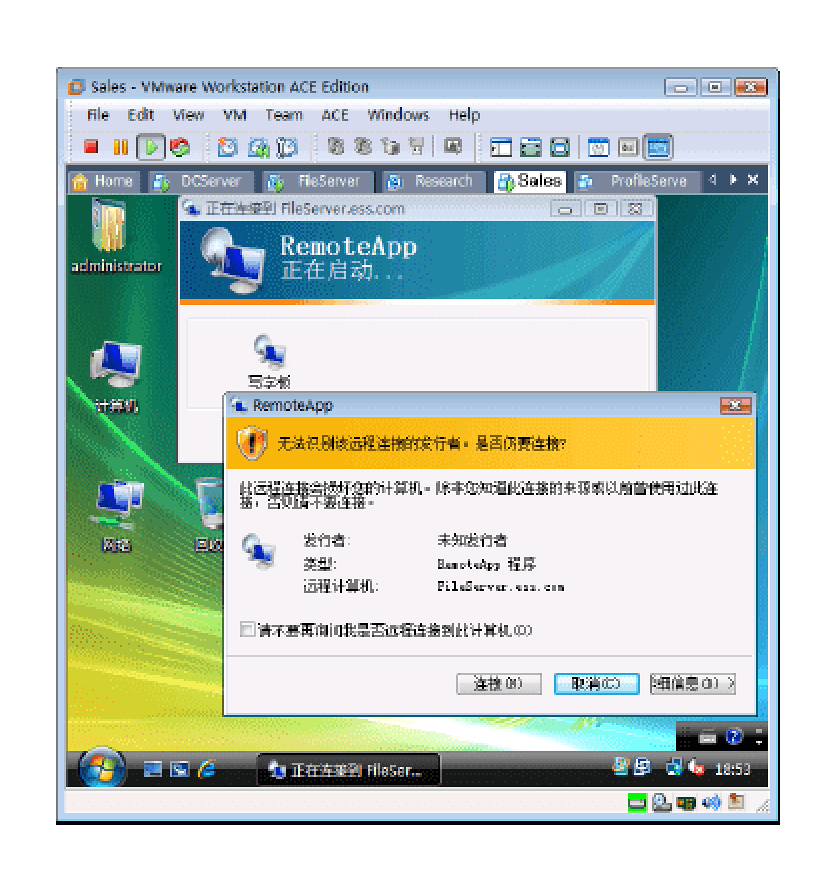


图 12-111　运行 RemoteApp

12.8　使用终端服务网关访问终端服务

终端服务网关(TS 网关)是这样一种类型的网关，它允许授权用户使用 Internet 连接从任何计算机连接到企业网络上的远程计算机。TS 网关使用远程桌面协议 (RDP) 和 HTTPS 帮助创建更安全的加密连接。

以下将会演示在 Research 计算机上安装终端服务网关角色，Workgroup 计算机使用终端服务网关 Research 访问到内网的终端服务 FileServer 以及启用了远程桌面的 DCServer 和 ProfileServer，实验环境如图 12-112 所示。需要在 DCServer 上安装企业 CA，为 Research 服务器颁发证书。

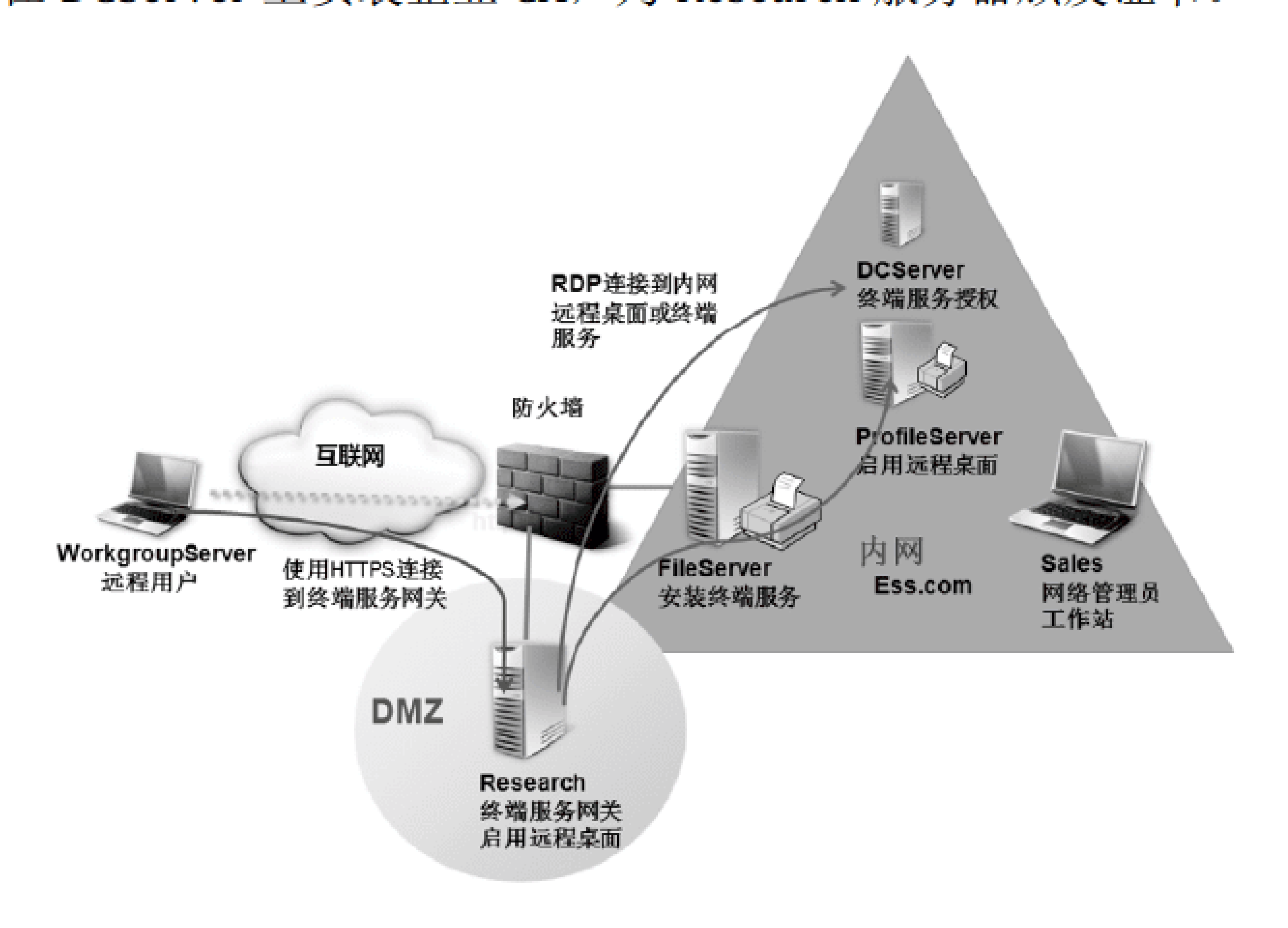


图 12-112　实验环境

12.8.1　任务 1：安装企业 CA

这个任务为配置 TS 网关做准备，因为 TS 网关配置 SSl 需要数字证书。安装一个企业 CA 为域中的用户和计算机颁发数字证书。

① 以域管理员的身份登录到 DCServer，如图 12-113 所示，打开服务器管理器，单击“添加角色”

按钮。

② 如图 12-114 所示，在“开始之前”界面中，单击“下一步”按钮。

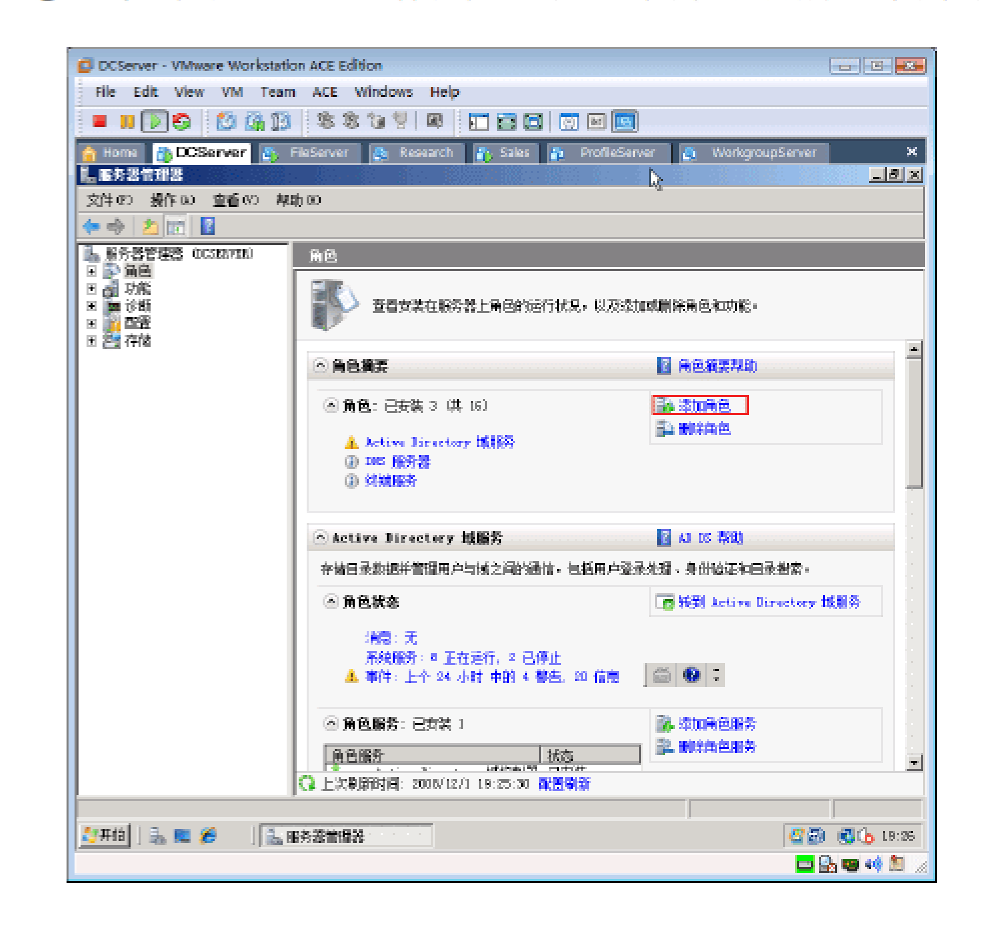


图 12-113　安装角色

图 12-114　安装向导

③ 如图 12-115 所示，在出现的“选择服务器角色”界面中，选中“Active Directory 证书服务”复选框，单击“下一步”按钮。

④ 如图 12-116 所示，在出现的“Active Directory 证书服务简介”对话框中，单击“下一步”按钮。

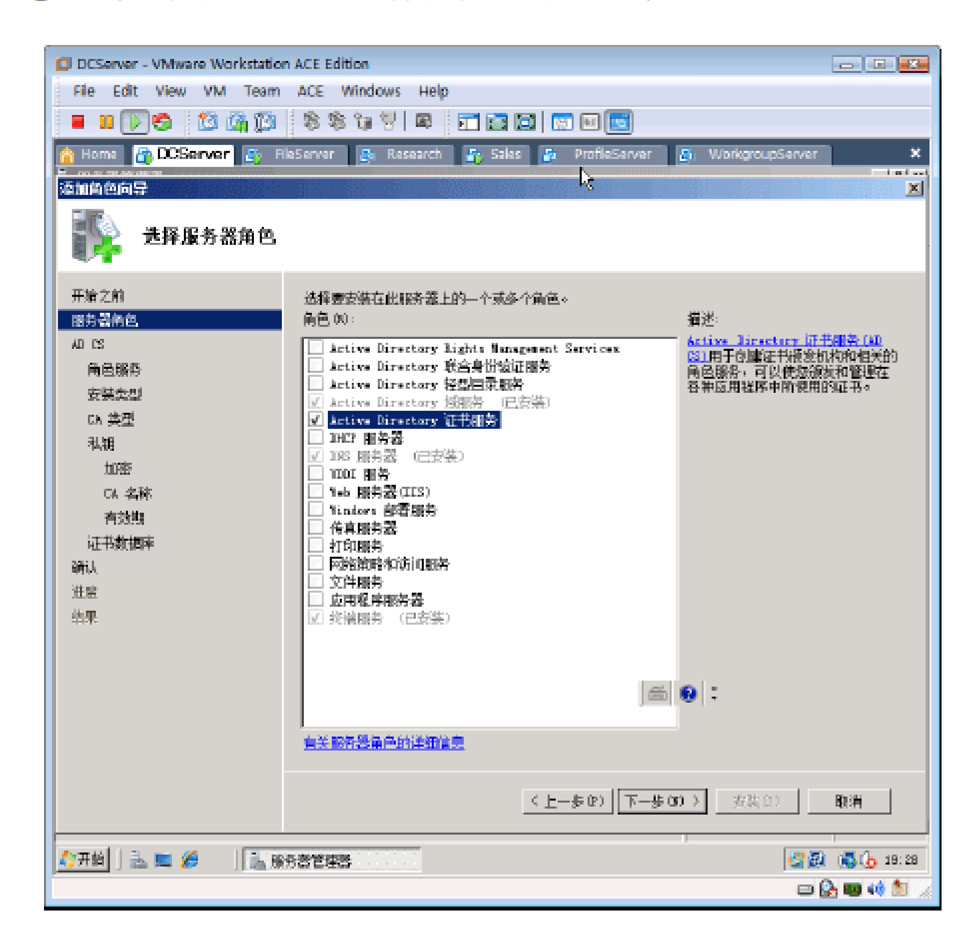


图 12-115　选择角色

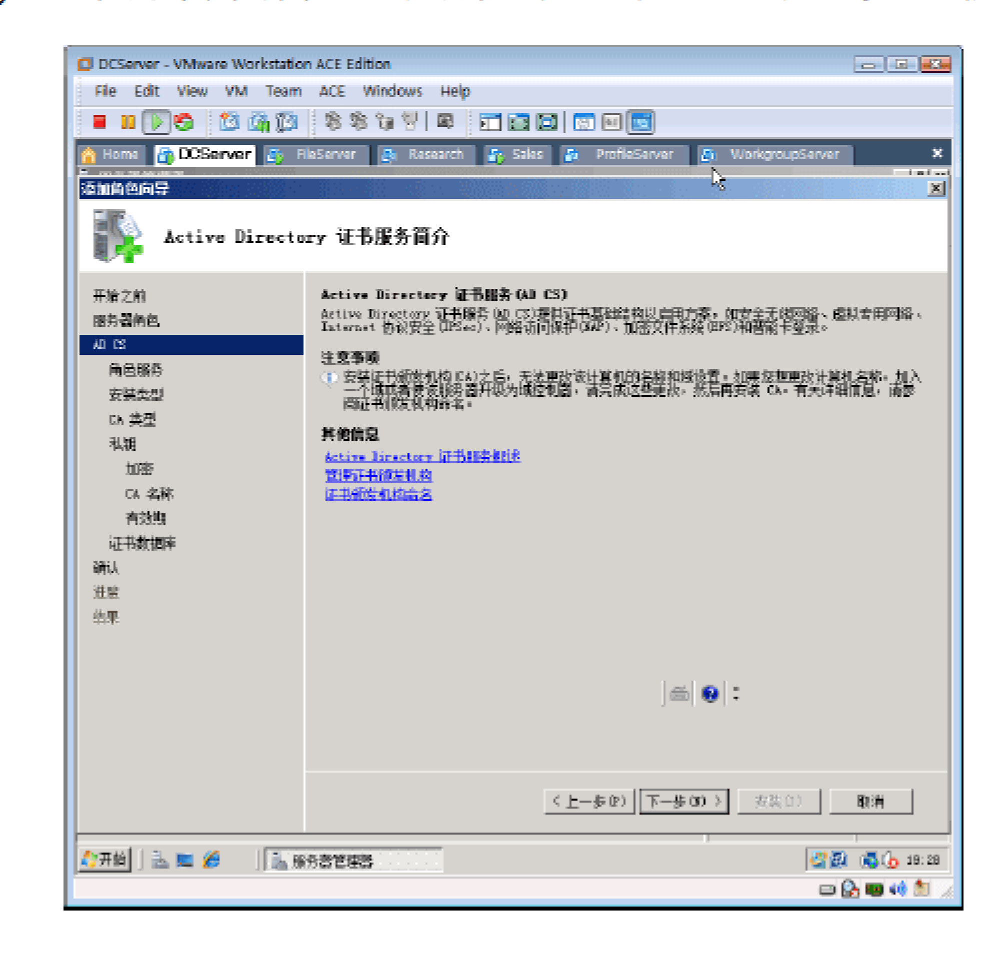


图 12-116　证书服务简介

⑤ 如图 12-117 所示，在“选择角色服务”界面中，选中“证书颁发机构”、“证书颁发机构 Web 注册”和“联机响应程序”复选框，在出现的“添加角色向导”对话框中，单击“添加必需的角色服务”按钮，单击“下一步”按钮。

⑥ 如图 12-118 所示，在“指定安装类型”界面中，选中“企业”单选按钮，单击“下一步”按钮。

⑦ 如图 12-119 所示，在出现的“指定 CA 类型”界面中，选中“根”单选按钮，单击“下一步”按钮。

⑧ 如图 12-120 所示，在出现的“设置私钥”对话框中，选中“新建私钥”单选按钮，单击“下一步”按钮。

⑨ 如图 12-121 所示，在出现的“为 CA 配置加密”对话框中，单击“下一步”按钮。

⑩ 如图 12-122 所示，在出现的“配置 CA 名称”对话框中，保持默认的名称，单击“下一步”按钮。



图 12-117　安装角色服务

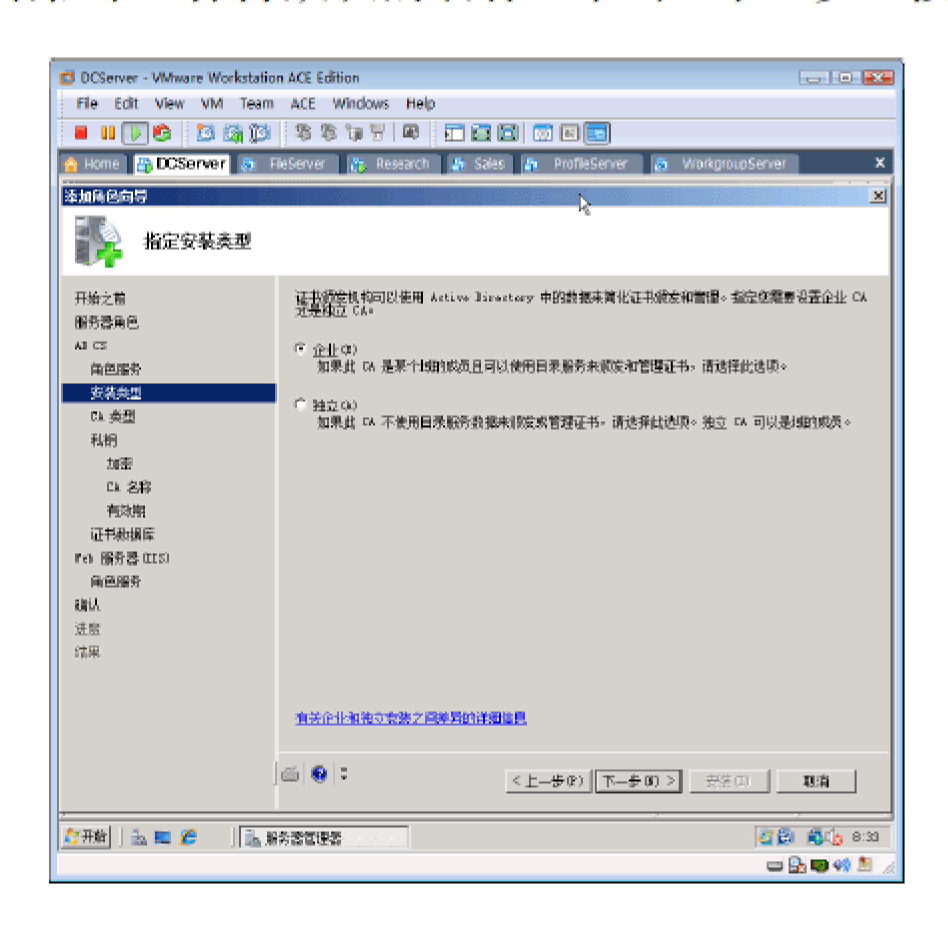


图 12-118　指定安装类型

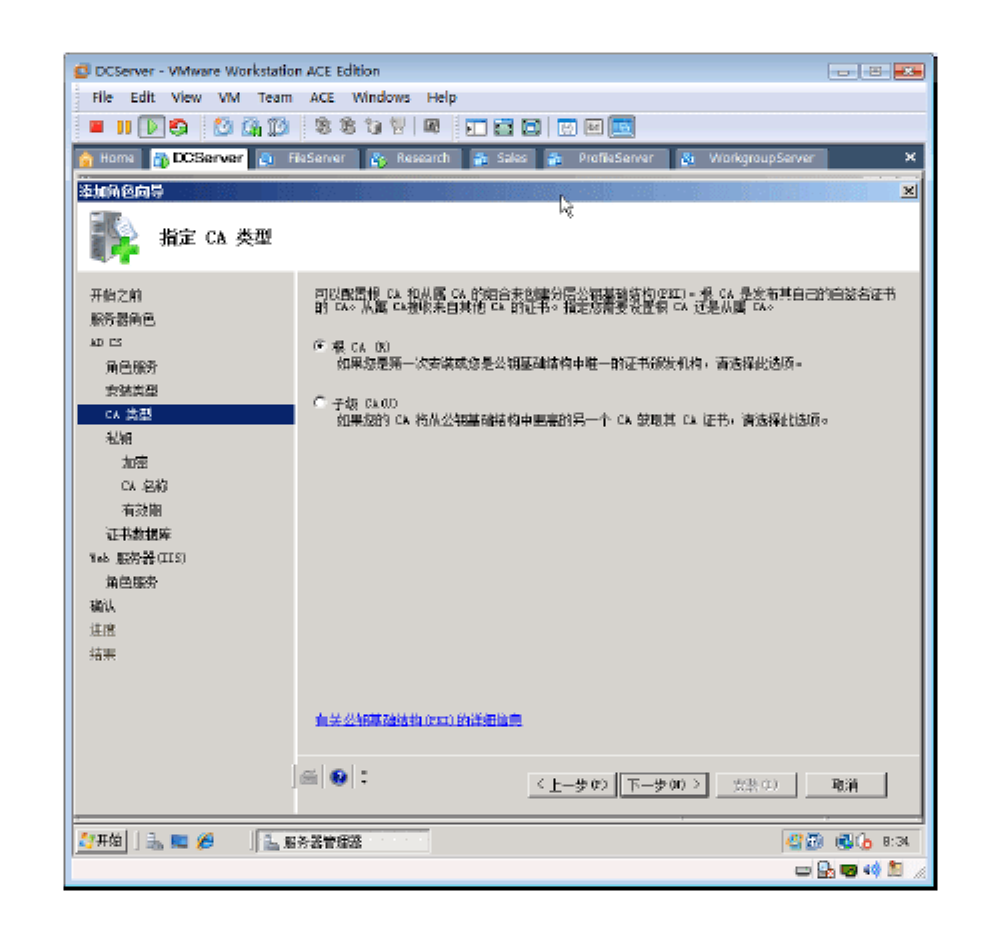


图 12-119　指定 CA 类型

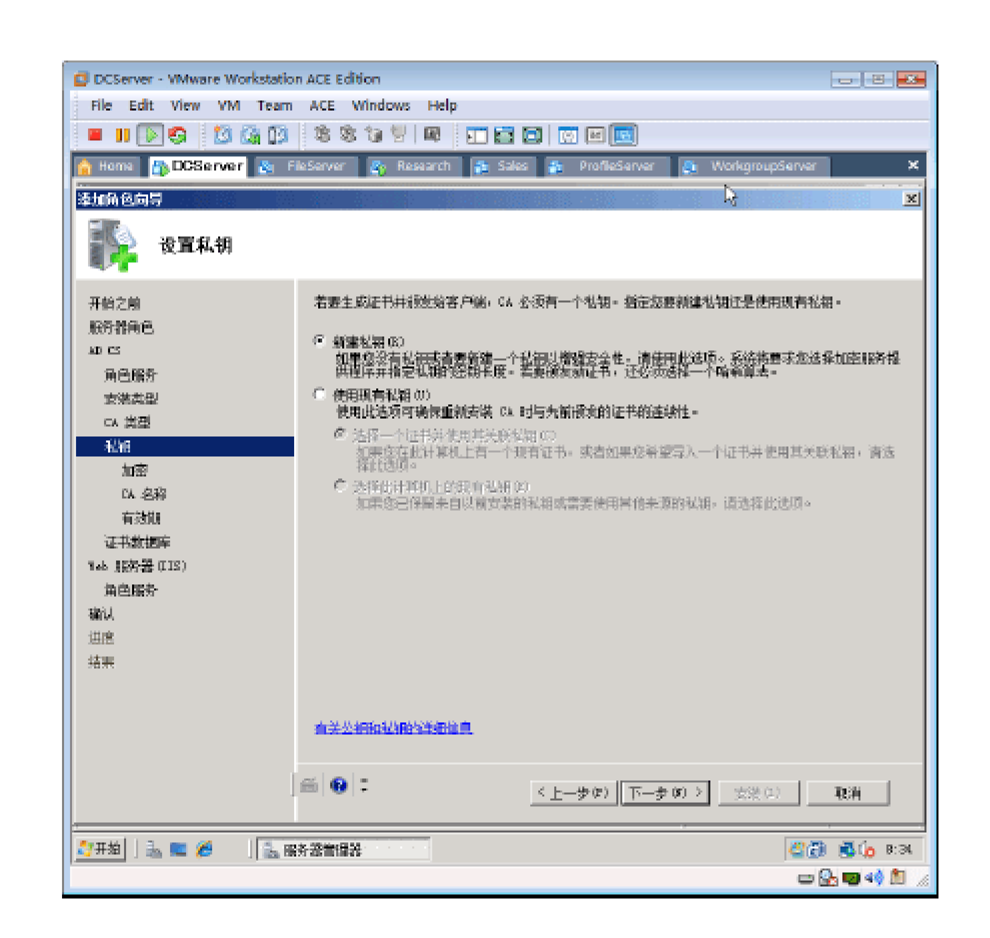


图 12-120　设置私钥

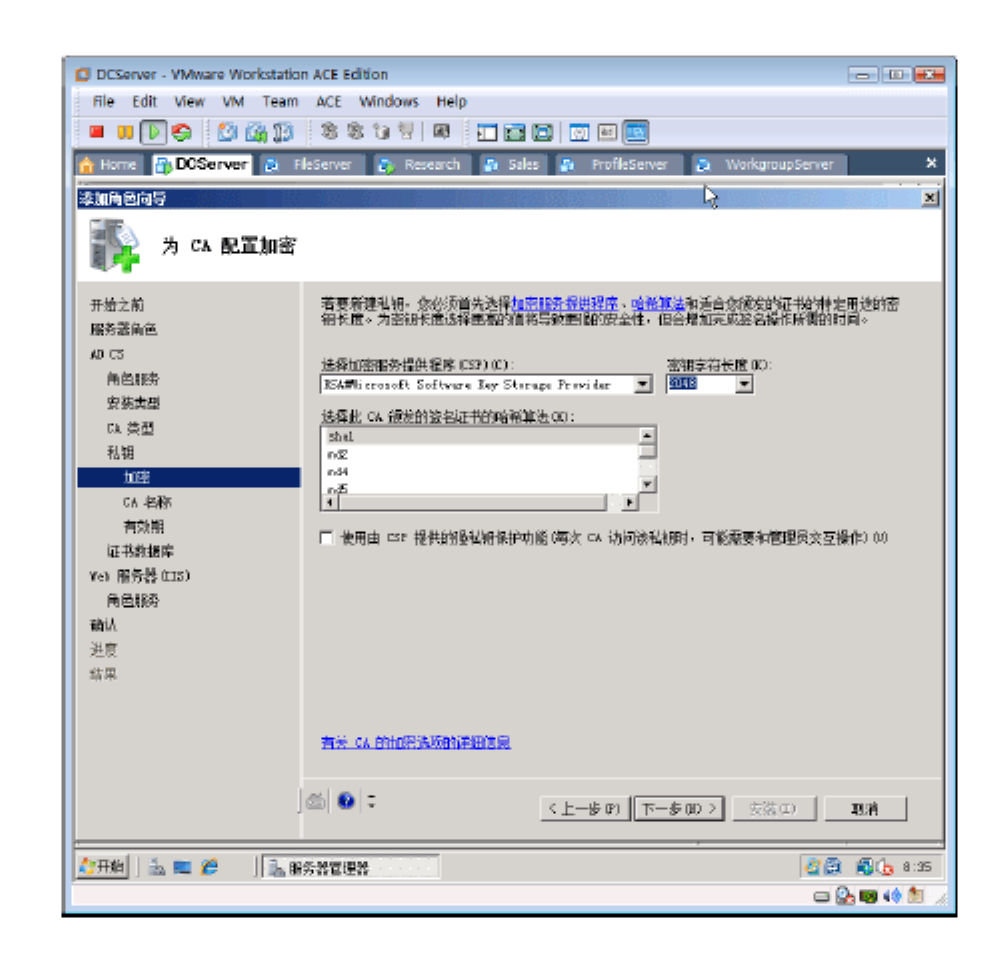


图 12-121　配置 CA 加密

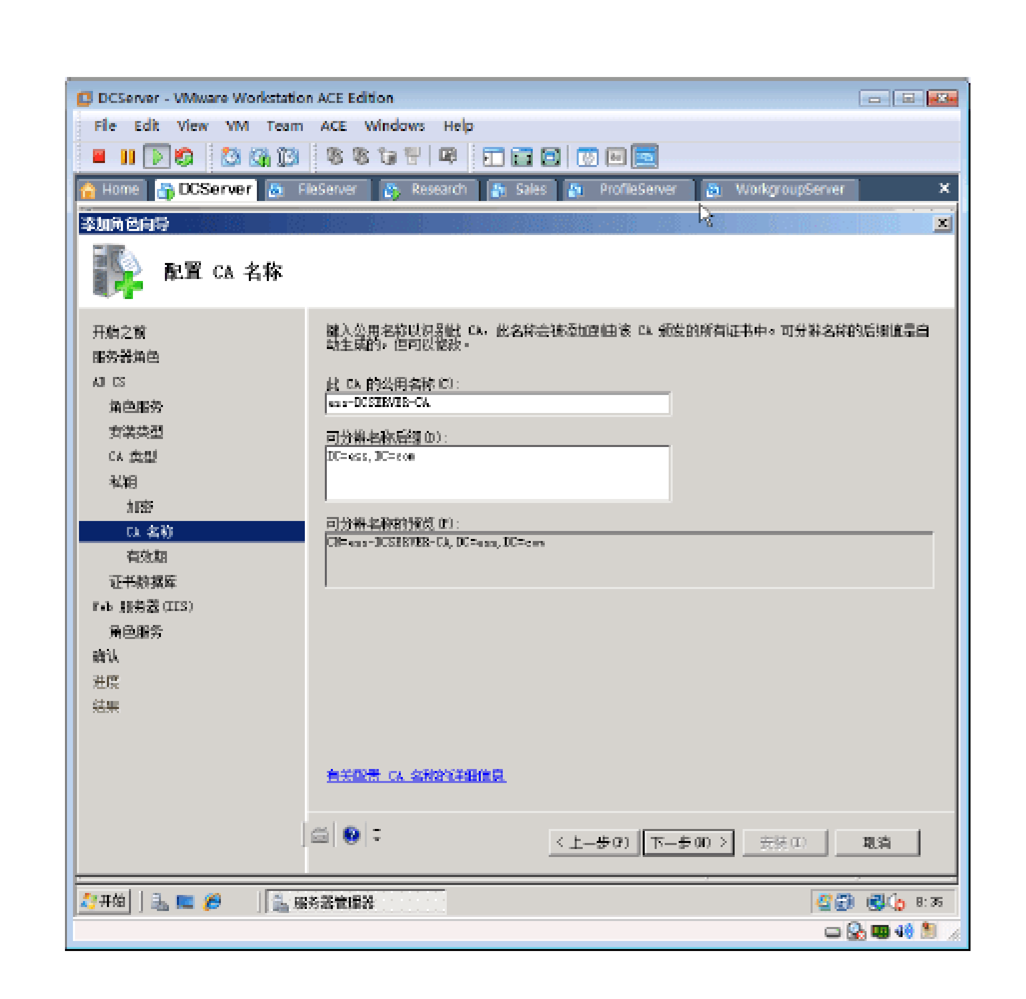


图 12-122　配置 CA 名称

⑪　如图 12-123 所示，在出现的“设置有效期”对话框中，单击“下一步”按钮。

⑫　如图 12-124 所示，在出现的“配置证书数据库”对话框中，单击“下一步”按钮。

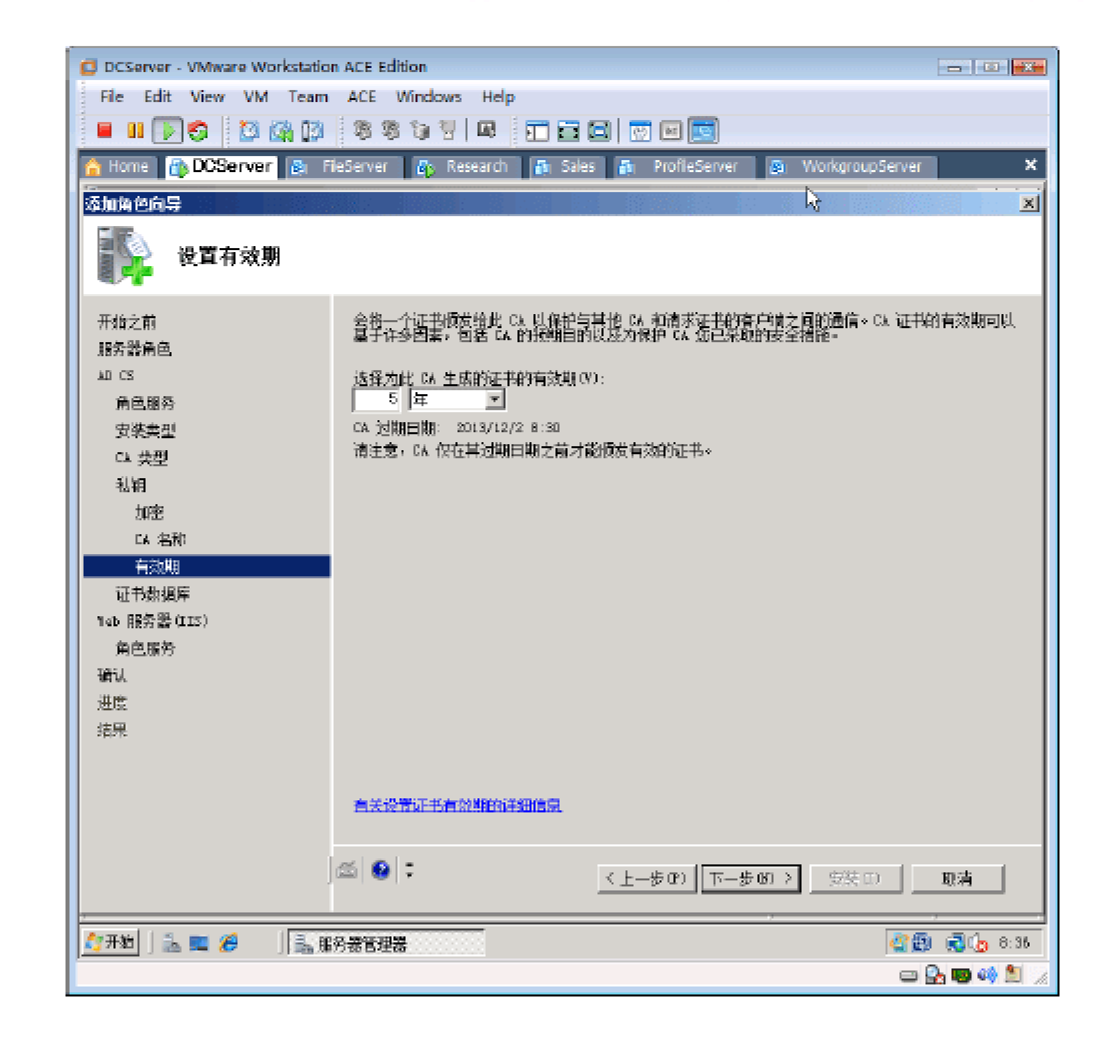


图 12-123　设置有效期

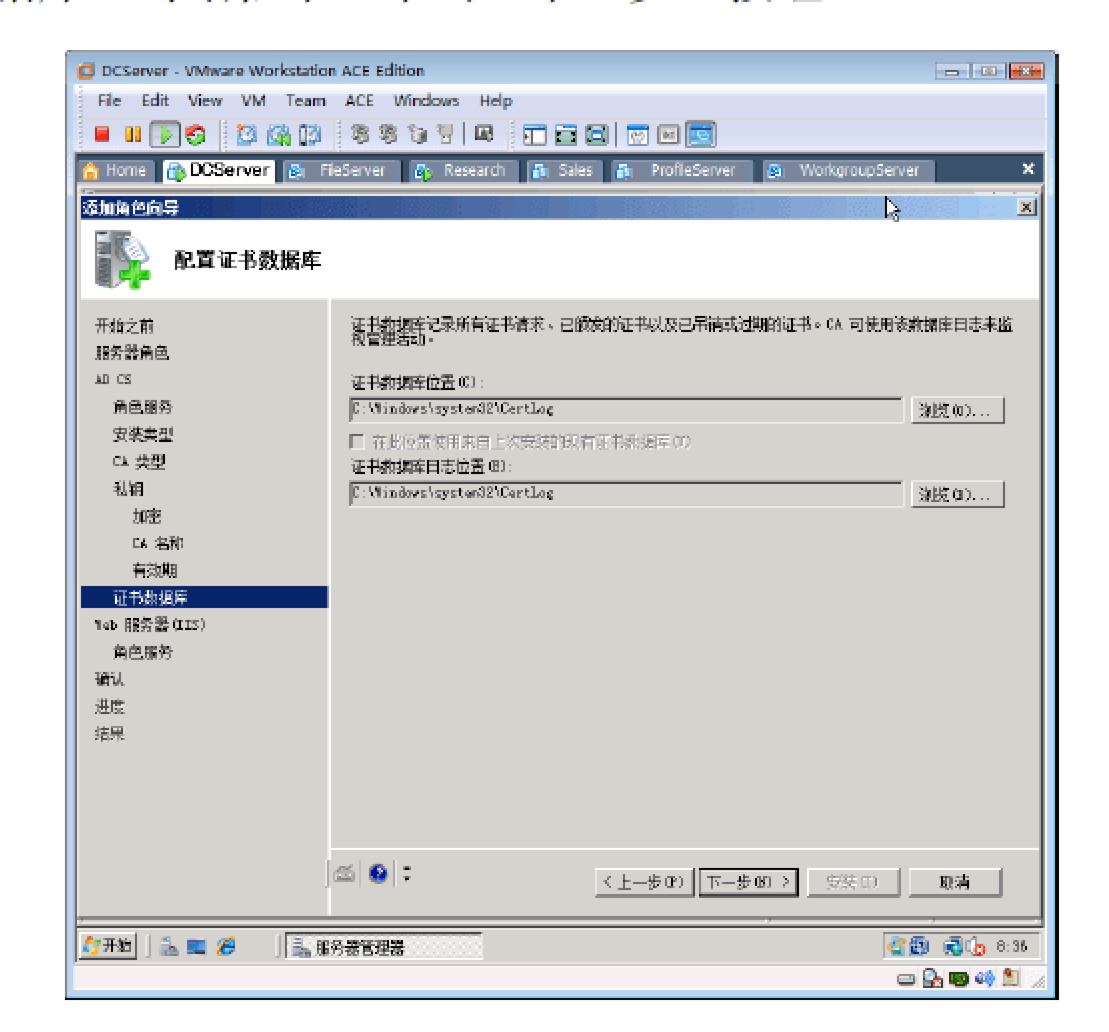


图 12-124　配置证书数据库

⑬　如图 12-125 所示，在出现的“Web 服务器(IIS)”界面中，单击“下一步”按钮。

⑭　如图 12-126 所示，在出现的“选择角色服务”界面中，单击“下一步”按钮。

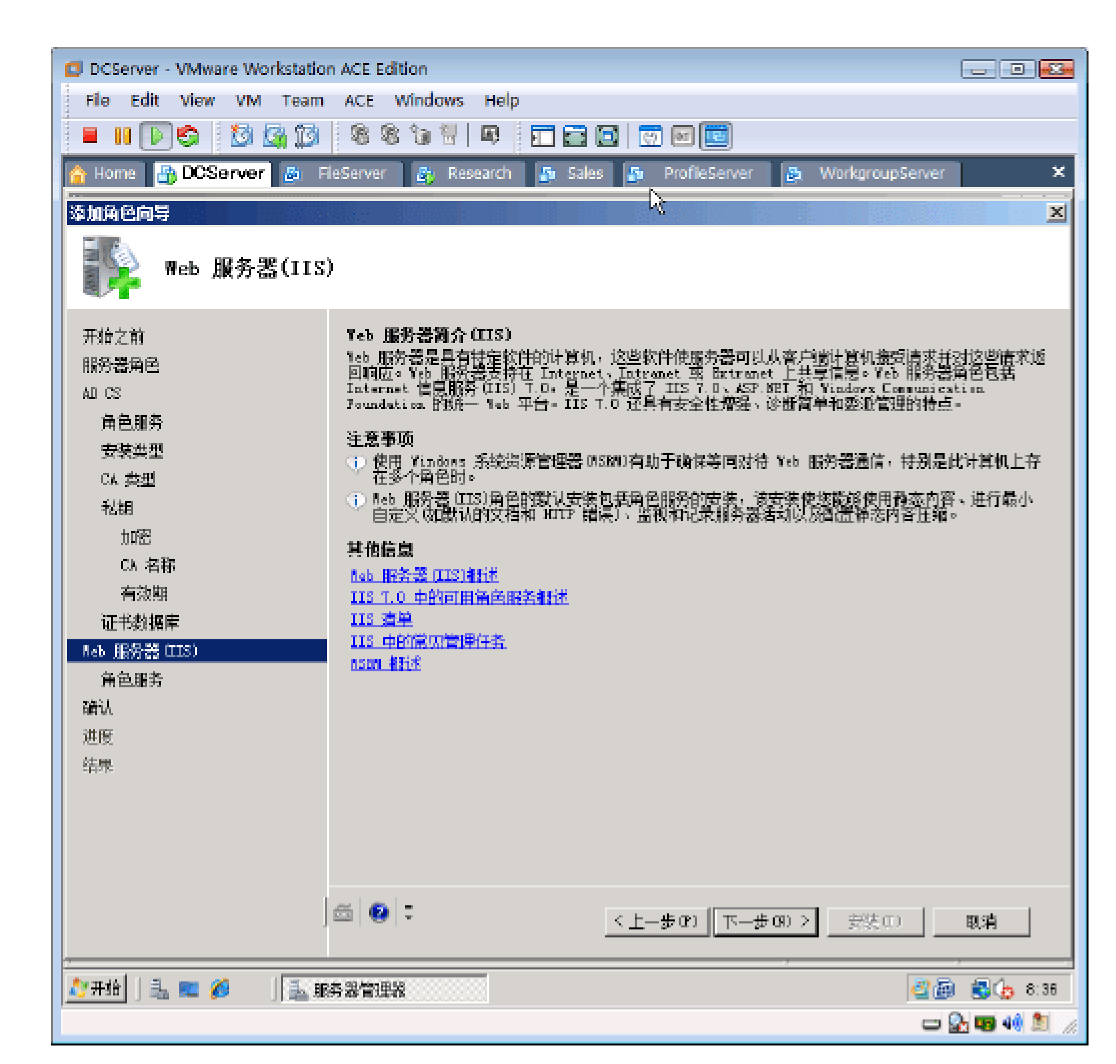


图 12-125　Web 服务器

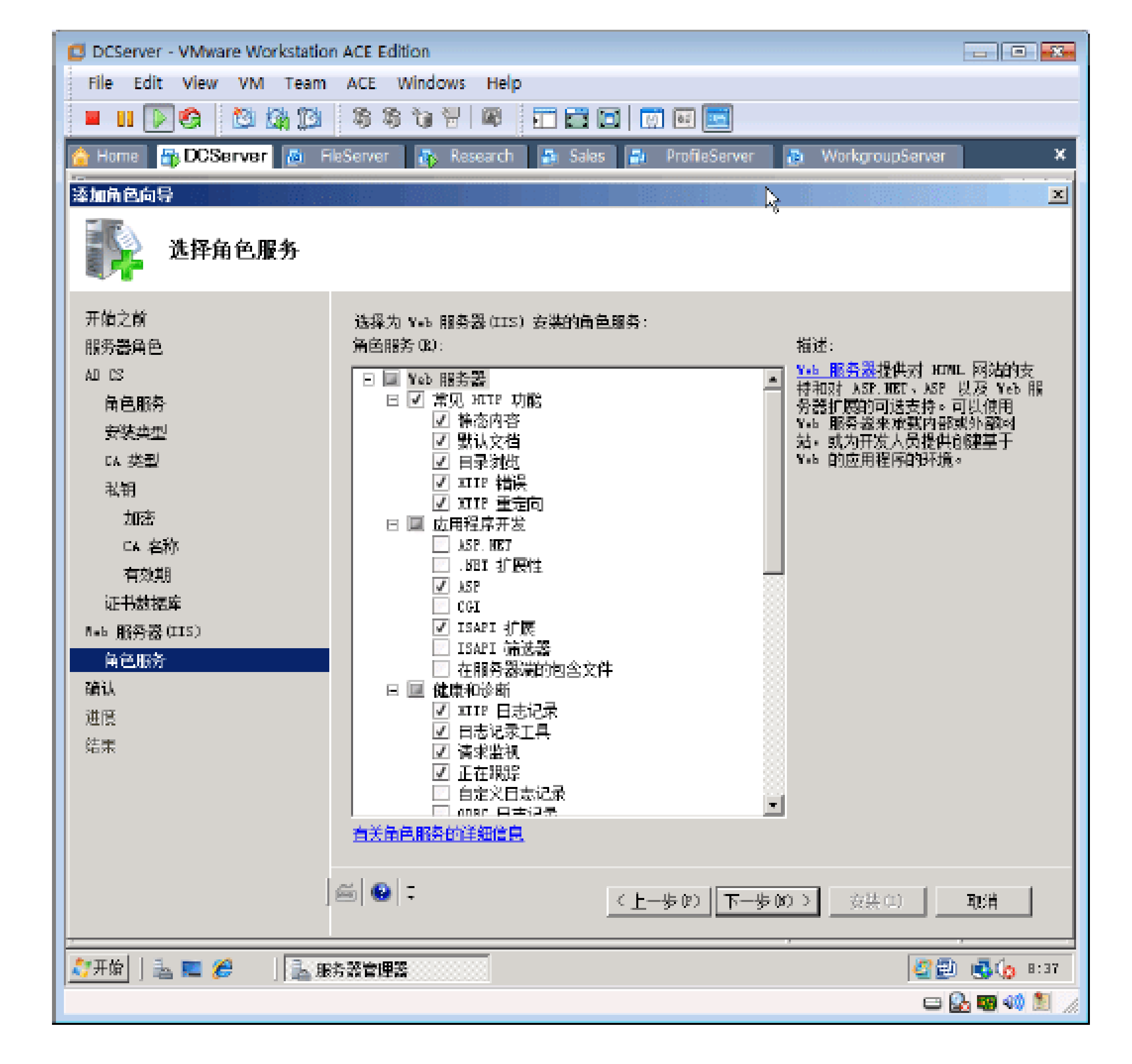


图 12-126　指定角色服务

⑮　如图 12-127 所示，在“确认安装选择”界面中，单击“安装”按钮，完成角色安装。

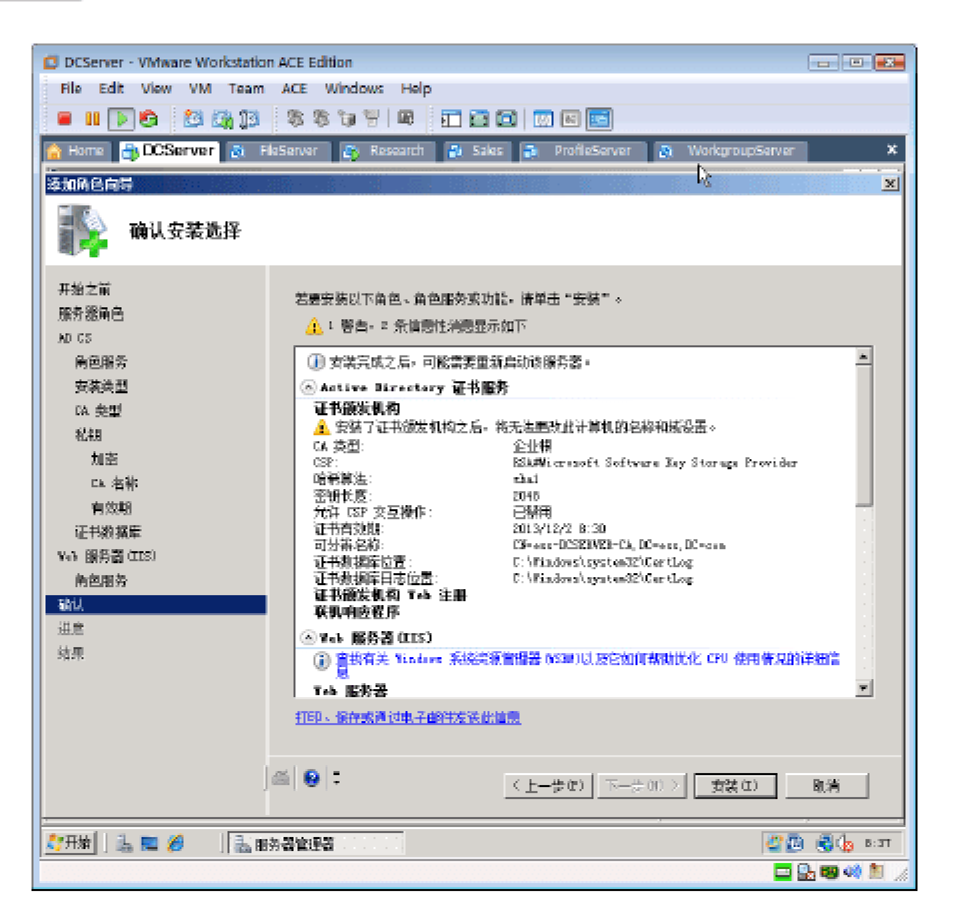


图 12-127　确认安装

12.8.2　任务 2：在 Research 上安装 TS 网关

① 以域管理员身份登录到 Research。

② 如图 12-128 所示，打开服务器管理器，单击“添加角色”按钮。

③ 如图 12-129 所示，在出现的“开始之前”界面中，单击“下一步”按钮。

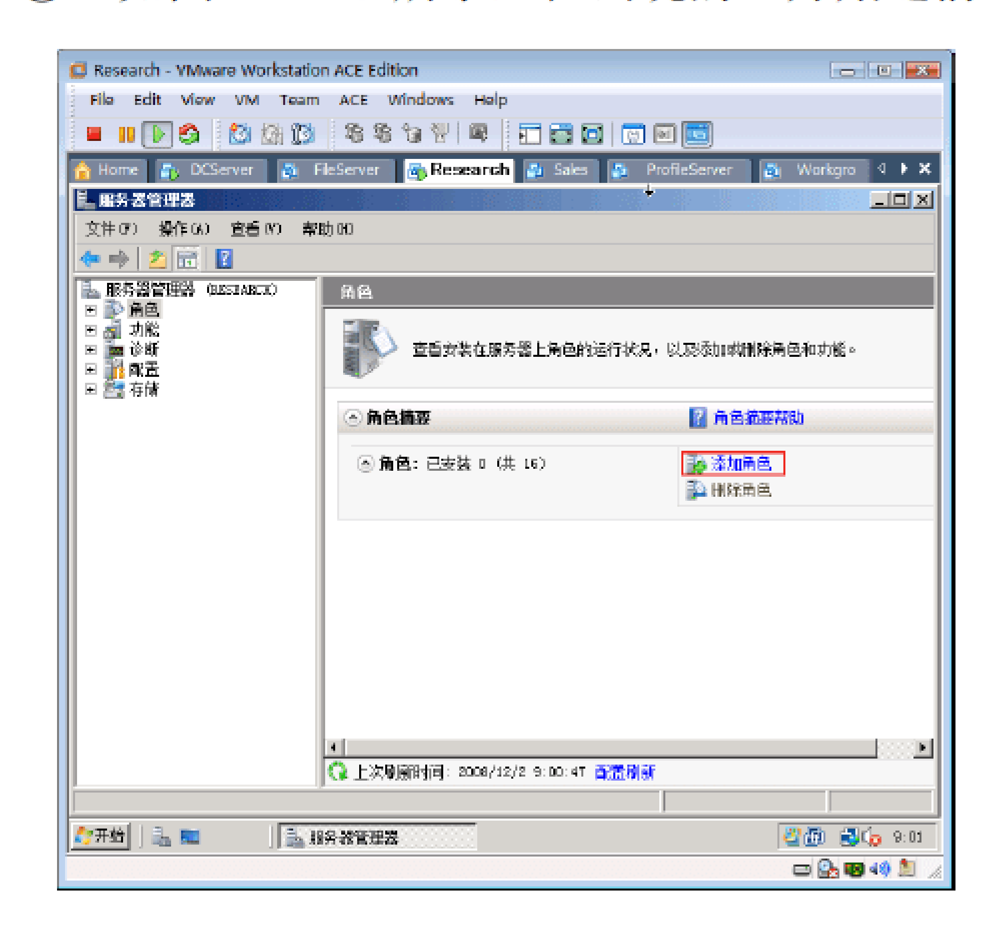


图 12-128　安装角色

图 12-129　安装向导

④ 如图 12-130 所示，在出现的“选择服务器角色”对话框中，选中“终端服务”复选框，单击“下一步”按钮。

⑤ 如图 12-131 所示，在出现的“终端服务”界面中，单击“下一步”按钮。

⑥ 如图 12-132 所示，在出现的“选择角色服务”界面中，选中“TS 网关”复选框，单击“下一步”按钮。

⑦ 如图 12-133 所示，在出现的“选择 SSL 加密的服务器身份验证证书”界面中，选中“稍后为 SSL 加密选择证书”单选按钮，单击“下一步”按钮。

⑧ 如图 12-134 所示，在出现的“为 TS 网关创建授权策略”界面中，选中“以后”单选按钮，单击“下一步”按钮。

⑨　如图 12-135 所示，在出现的“网络策略和访问服务”界面中，单击“下一步”按钮。

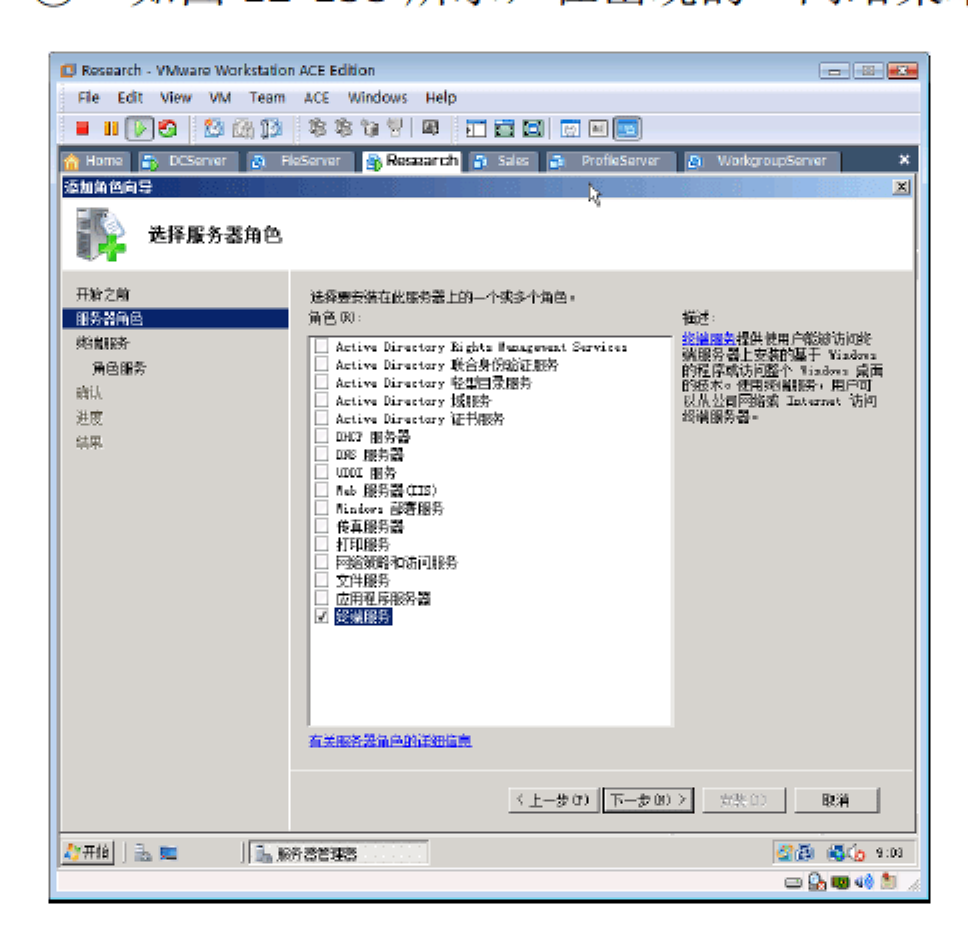


图 12-130　选择角色

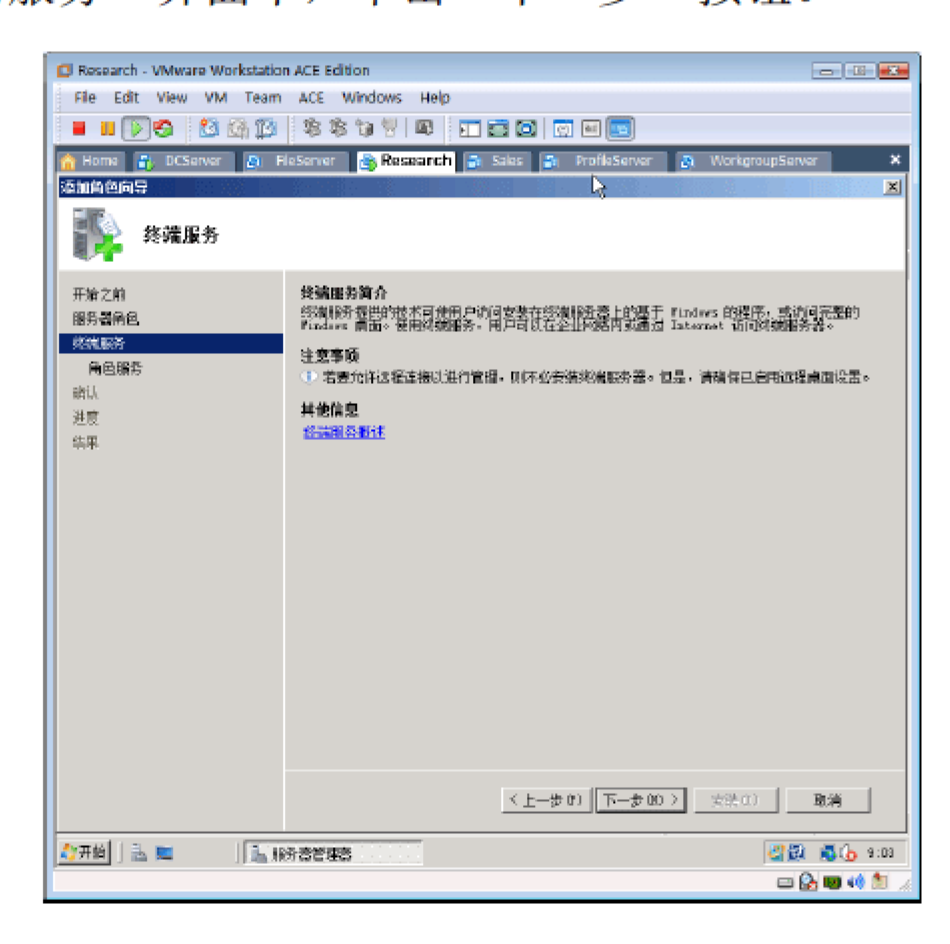


图 12-131　终端服务介绍

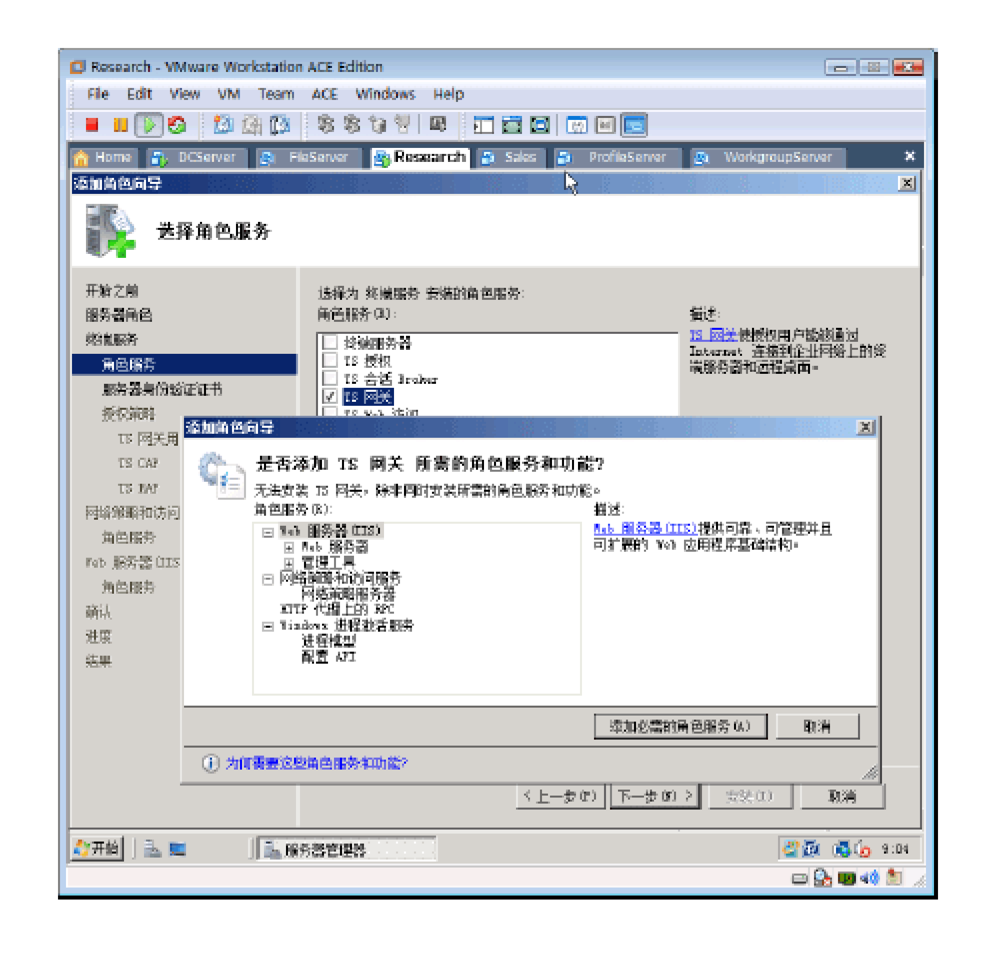


图 12-132　选择角色服务

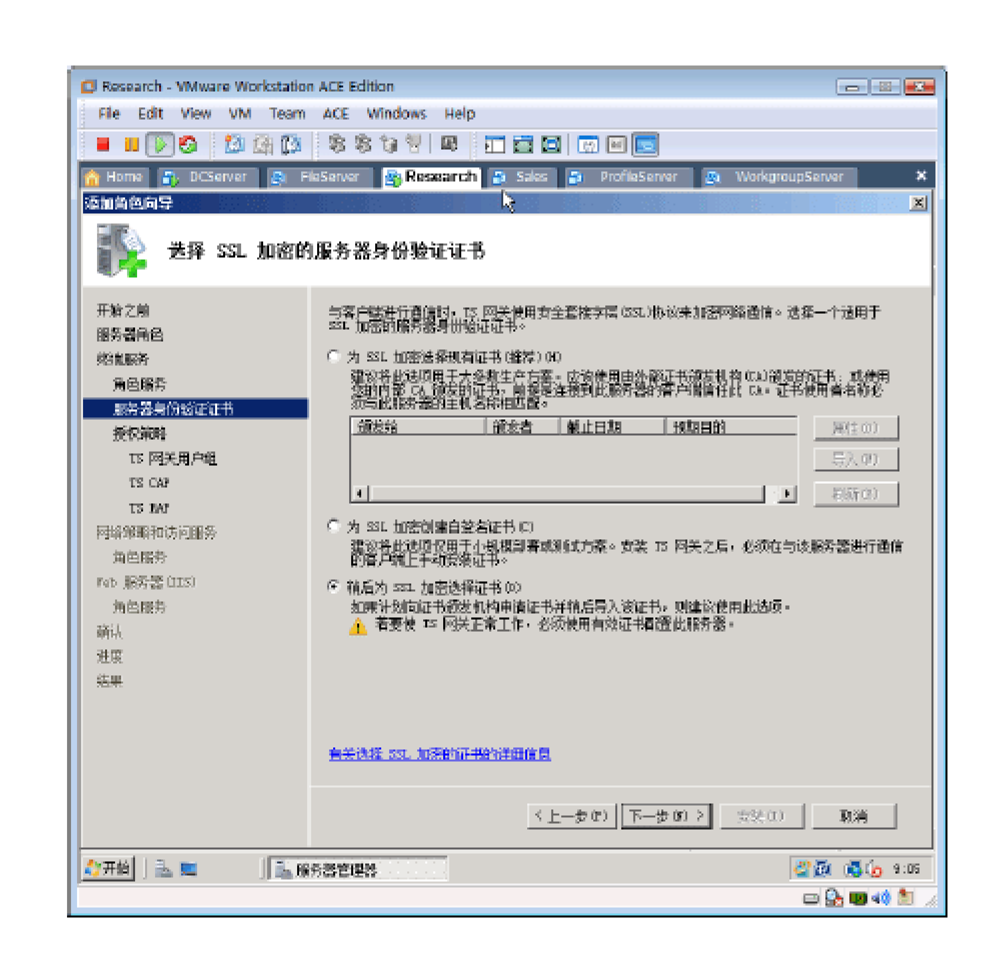


图 12-133　选择证书

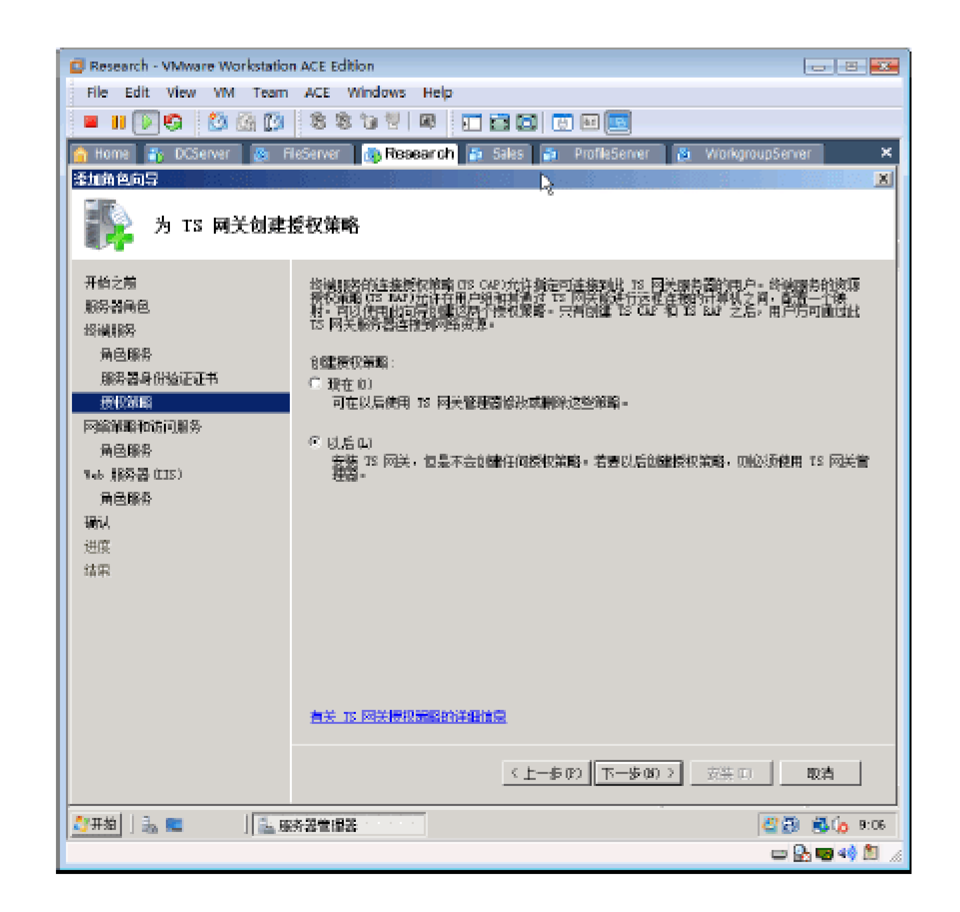


图 12-134　创建授权策略

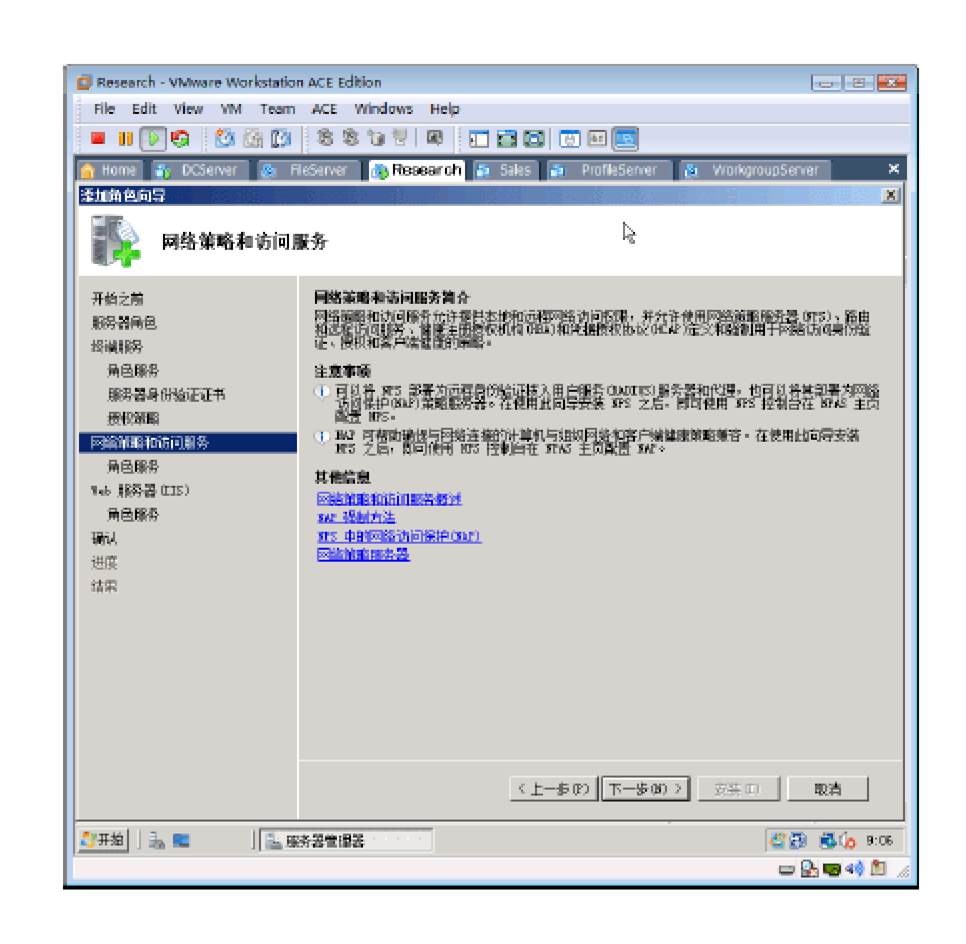


图 12-135　网络策略和访问服务介绍

⑩ 如图 12-136 所示，在出现的“选择角色服务”界面中，选中“网络策略服务器”复选框，单击“下一步”按钮。

⑪ 如图 12-137 所示，在出现的“Web 服务器(IIS)”对话框中，单击“下一步”按钮。

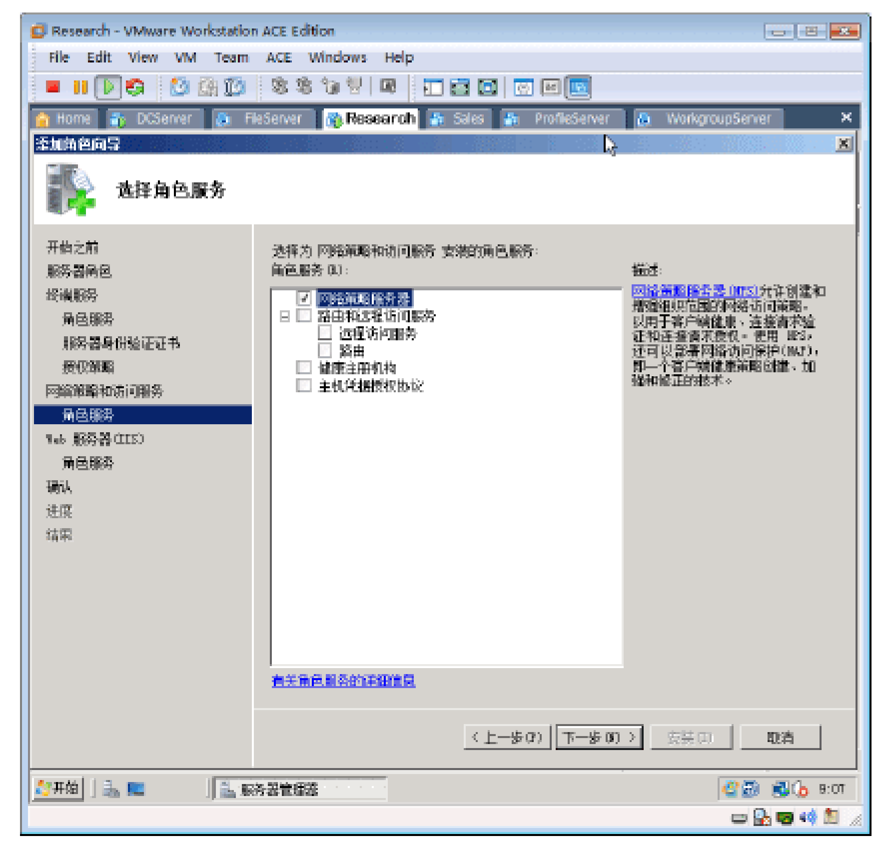


图 12-136　选择角色服务

图 12-137　IIS 介绍

⑫ 如图 12-138 所示，在出现的“选择角色服务”界面中，保持默认选择，单击“下一步”按钮。

⑬ 如图 12-139 所示，在出现的“确认安装选择”界面中，单击“安装”按钮。

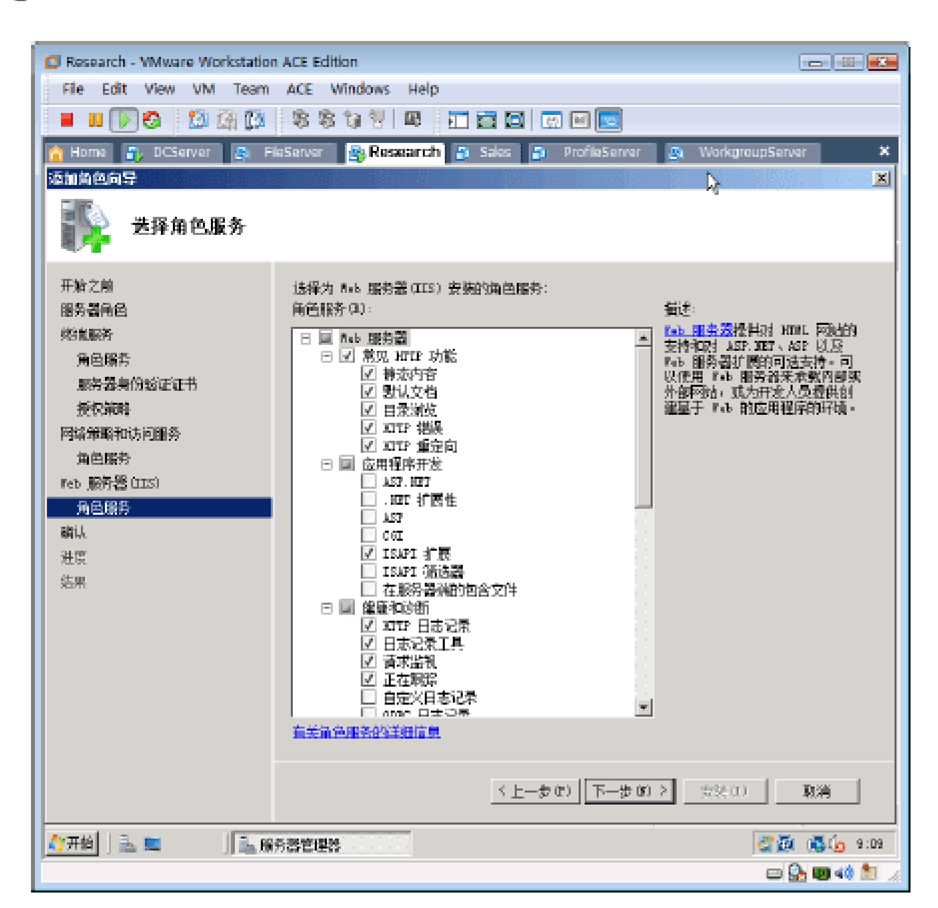


图 12-138　保持默认角色服务

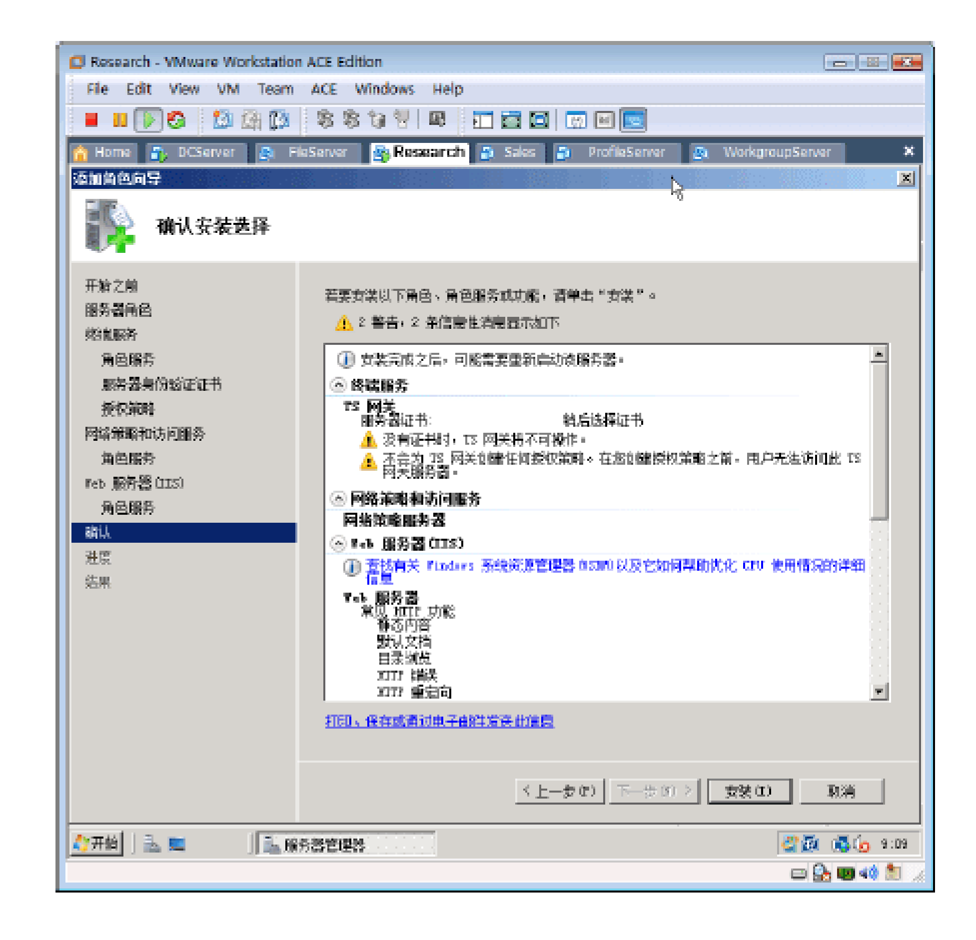


图 12-139　确认安装

12.8.3　任务 3：配置 TS 网关证书

下面介绍申请服务器证书，并配置 TS 网关使用该证书。

① 选择“开始”→“运行”命令，在出现的“运行”对话框中输入 gpupdate /force，单击“确定”按钮，刷新组策略。因为是刚刚安装的企业 CA，域中的计算机必须刷新组策略才能发现域中的 CA。

② 如图 12-140 所示，选择“开始”→“运行”命令，在出现的“运行”对话框中输入 mmc，单击“确定”按钮。

③ 如图 12-140 所示，在打开的控制台窗口中，选择“文件”→“添加/删除管理单元”命令。

④ 如图 12-141 所示，在出现的“添加或删除管理单元”对话框中，选中“证书”，单击“添加”按钮。

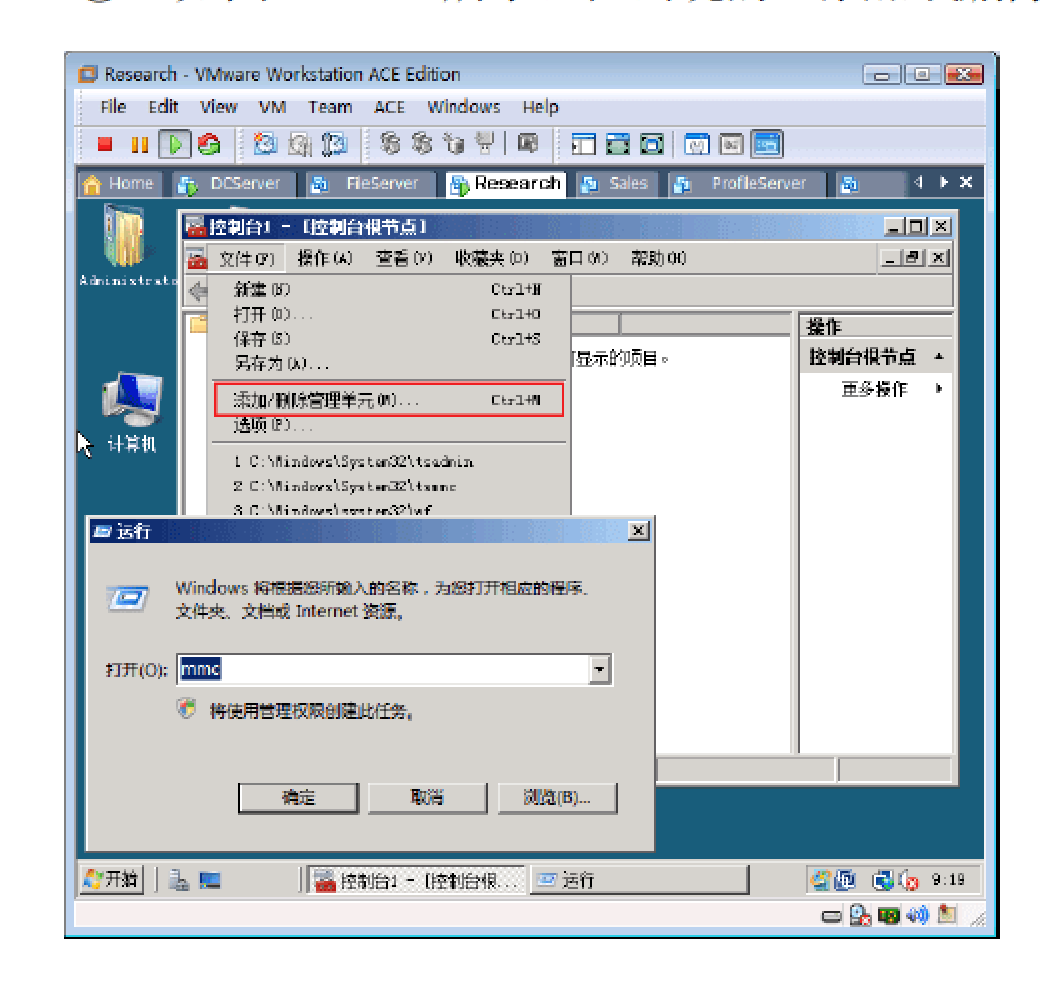


图 12-140 添加删除管理单元

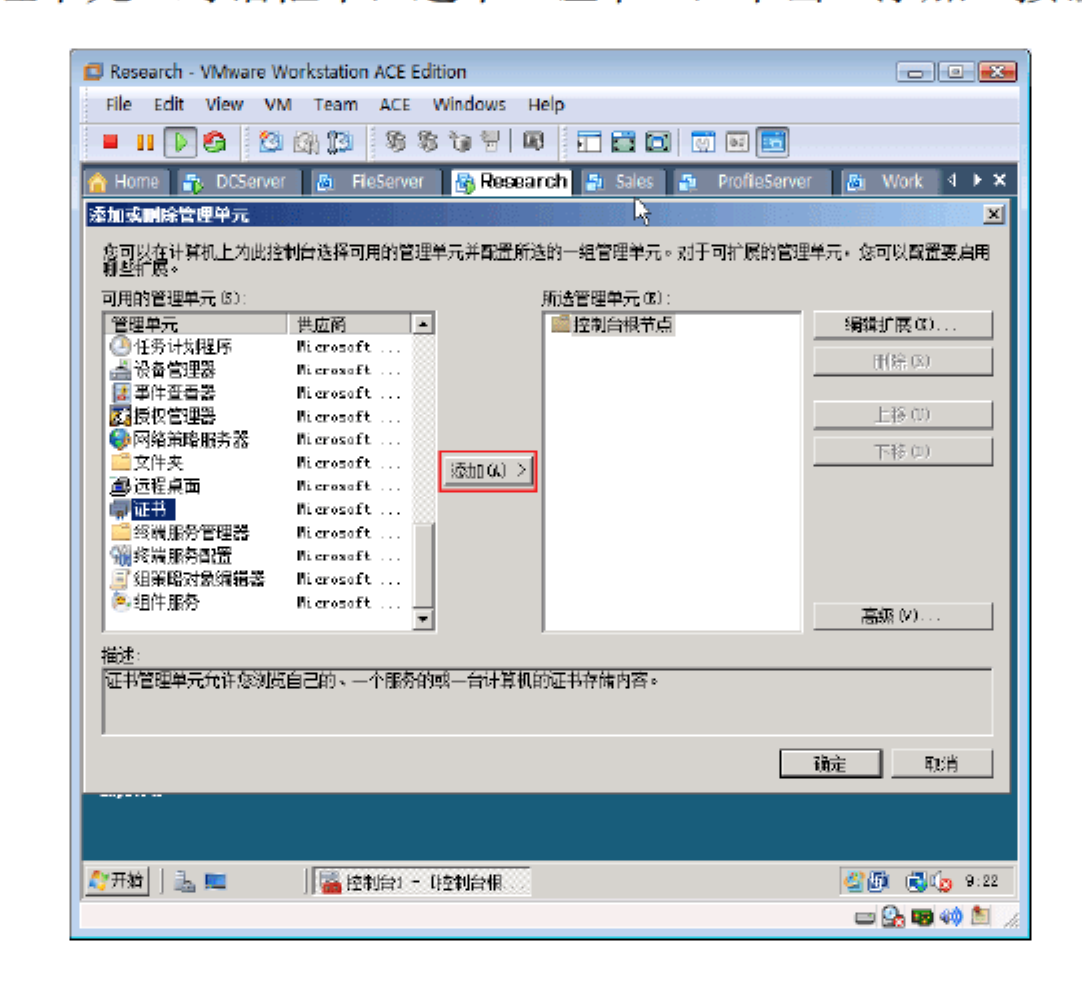


图 12-141 选择证书管理单元

⑤ 如图 12-142 所示，在“证书管理单元”对话框中，选中“计算机帐户”单选按钮，单击“下一步”按钮。

⑥ 如图 12-143 所示，在“选择计算机”对话框中，选中“本地计算机”单选按钮，单击“完成”按钮。

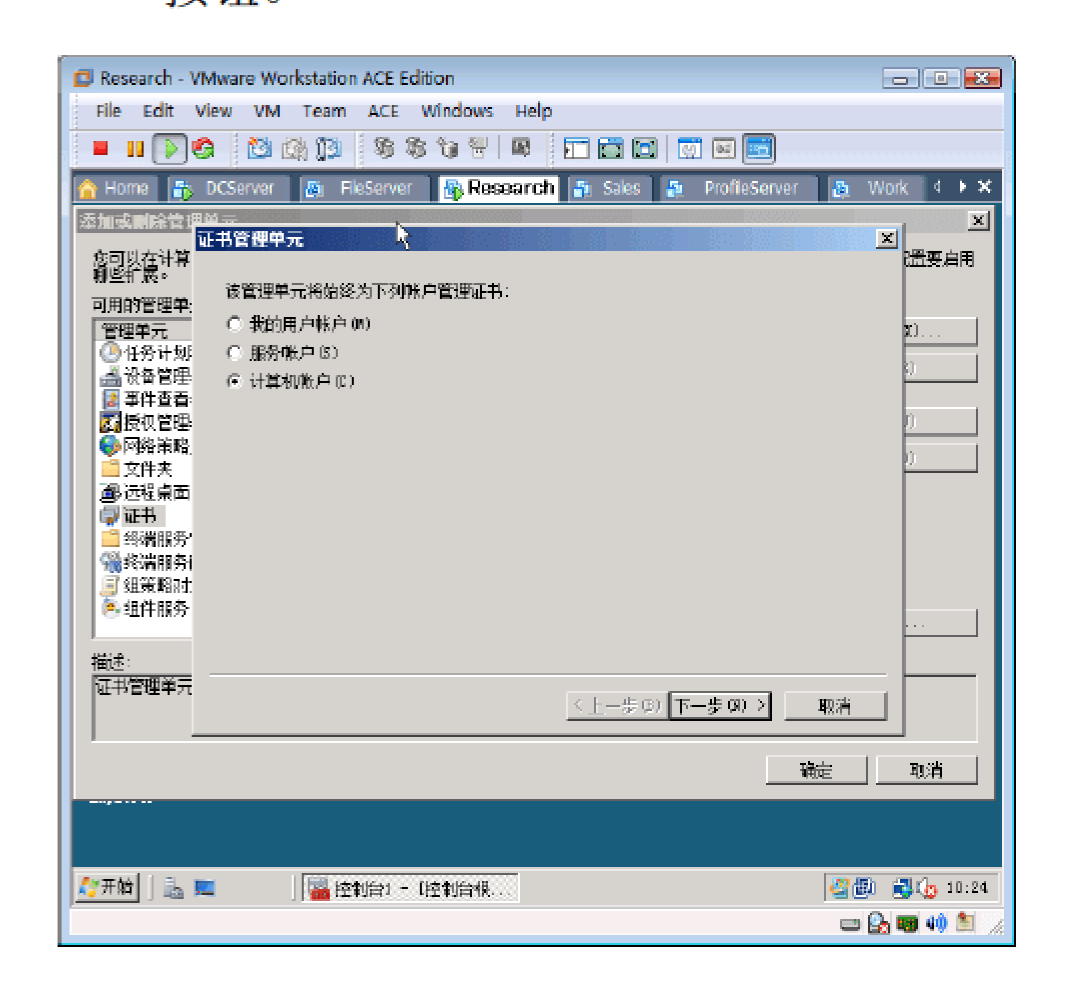


图 12-142 选择计算机

图 12-143 选择本地计算机

⑦ 如图 12-144 所示，右击“个人”，在弹出的快捷菜单中选择“所有任务”→“申请新证书”命令。

⑧ 如图 12-145 所示，在“在您开始前”对话框中，单击“下一步”按钮。

⑨ 如图 12-146 所示，在出现的“申请证书”界面中，选中“计算机”复选框，单击“注册”按钮。

⑩ 如图 12-147 所示，在“证书安装结果”界面中，单击“完成”按钮。

⑪ 如图 12-148 所示，展开“个人”→“证书”节点，可以看到刚才申请的证书。双击该证书，在“证书路径”选项卡中，可以看到是企业 CA 颁发的证书。

⑫ 选择“开始”→“程序”→“管理工具”→“终端服务”→“TS 网关管理”命令。

⑬ 如图 12-149 所示，在打开的“TS 网关服务器状态”界面中，单击“查看或修改证书属性”按钮。

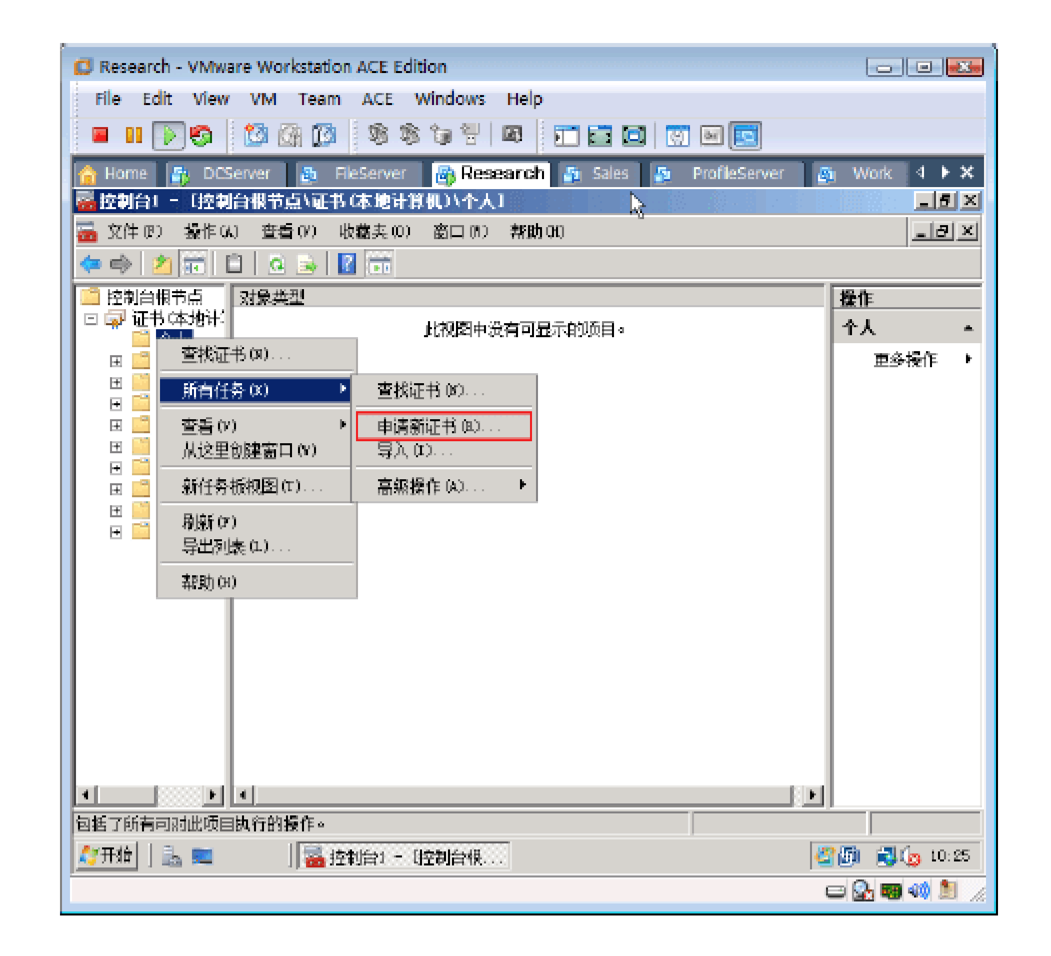


图 12-144　申请证书

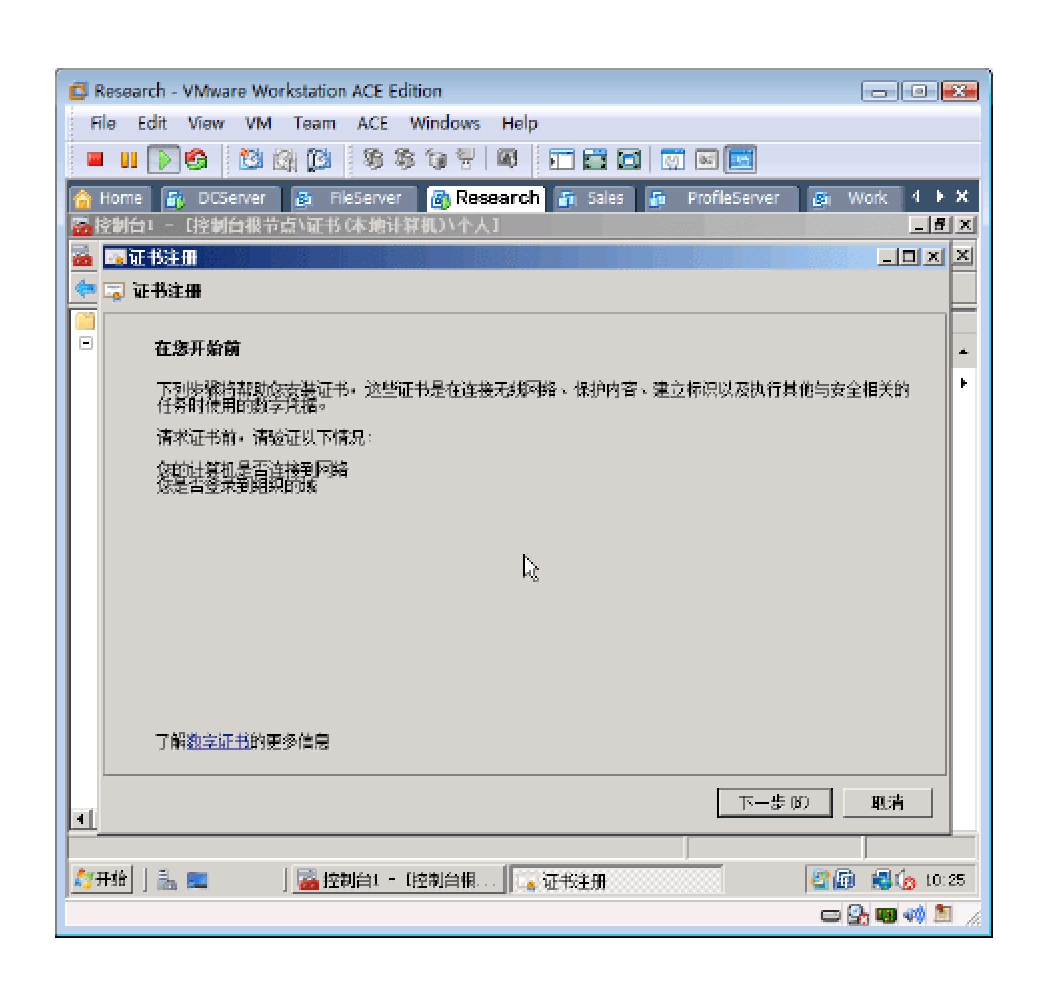


图 12-145　申请证书向导

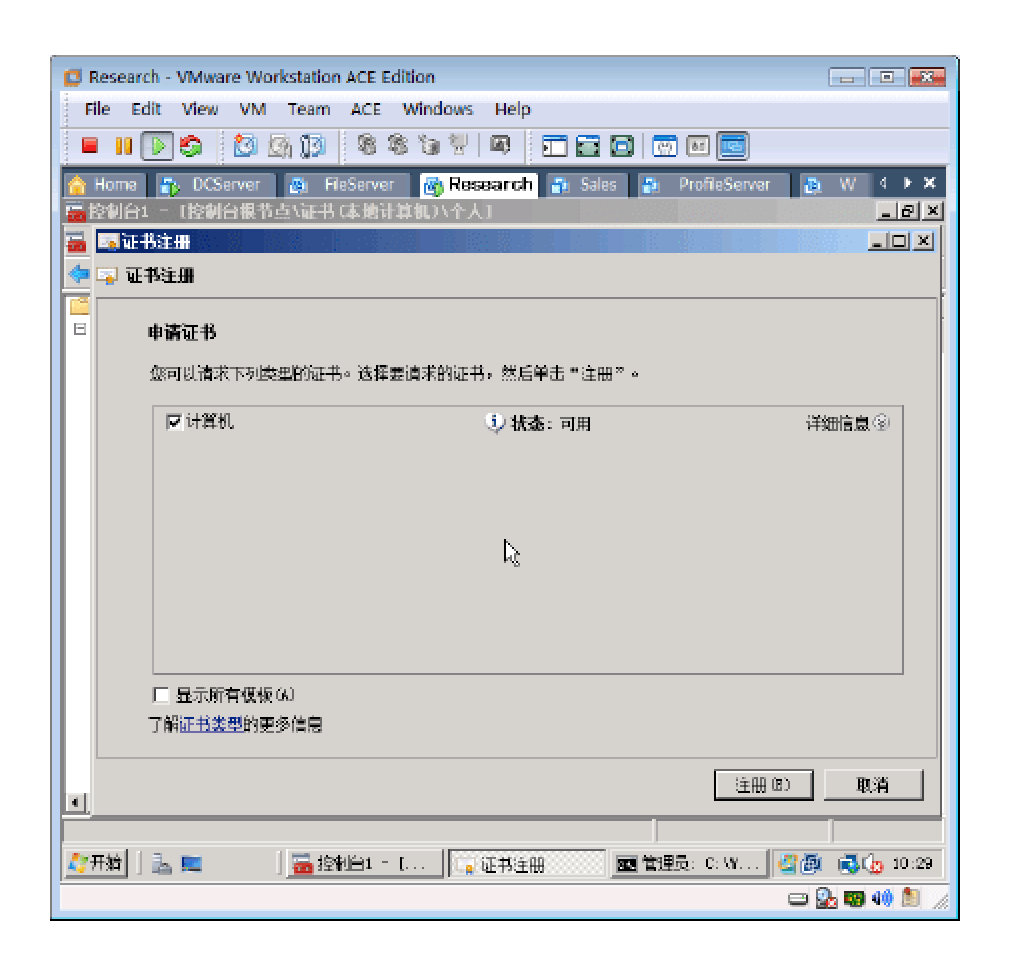


图 12-146　选择证书

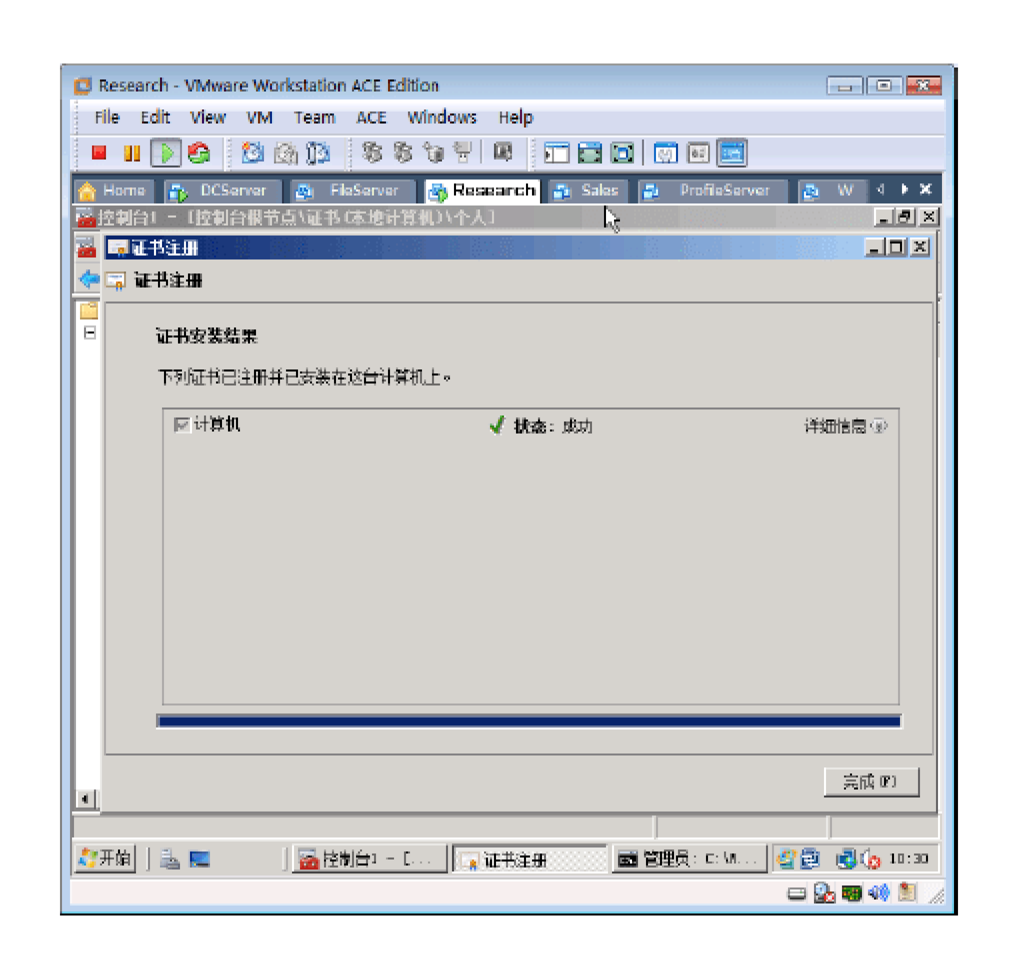


图 12-147　证书安装结果

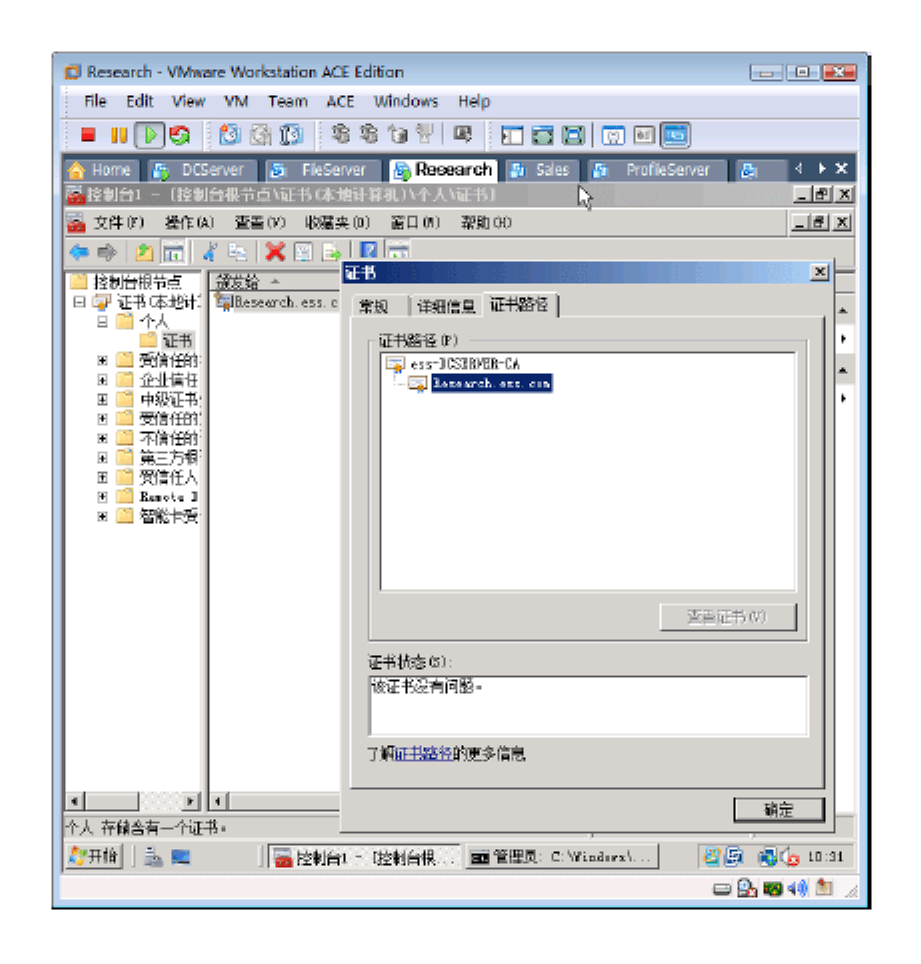


图 12-148　查看申请的证书

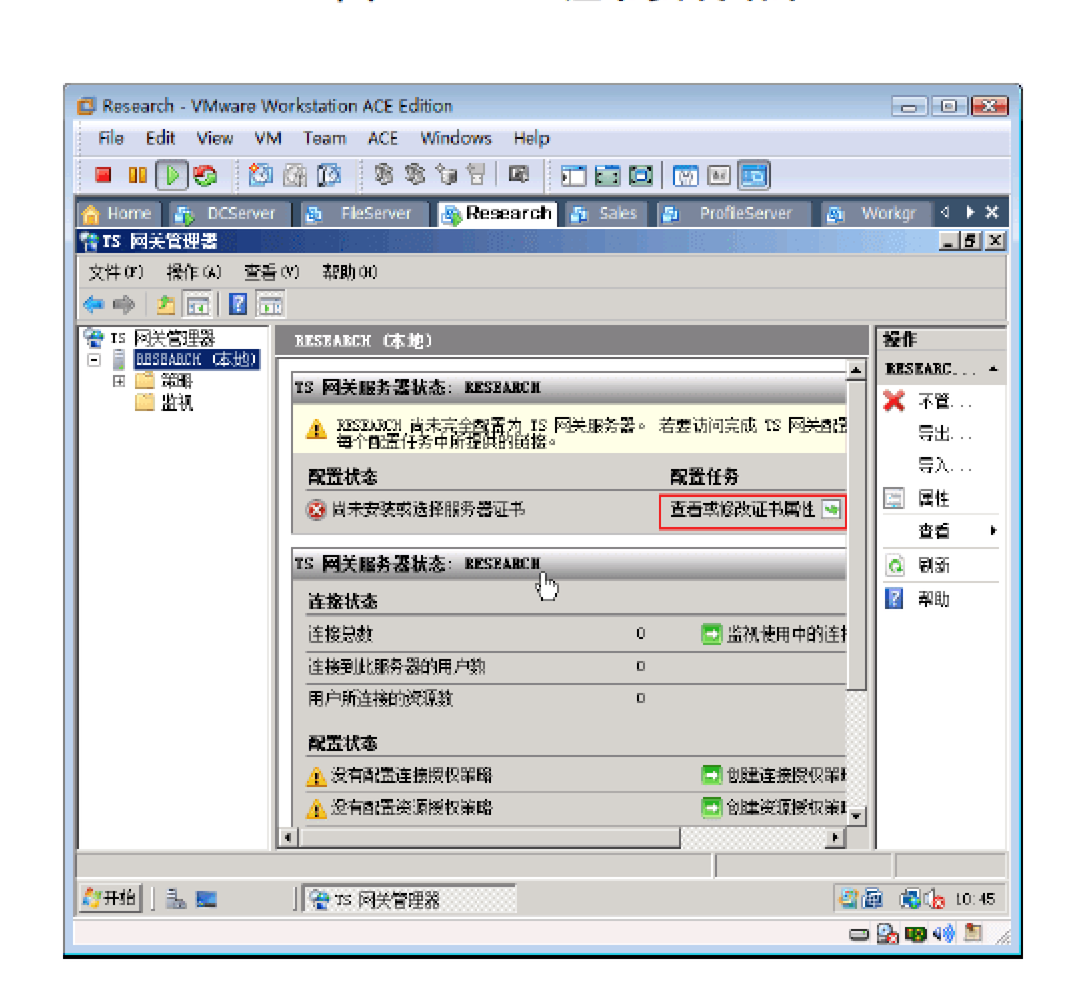


图 12-149　查看或修改证书属性

⑭　如图 12-150 所示，在“RESEARCH 属性”对话框的“SSL 证书”选项卡中，单击“浏览证书”按钮。

⑮　如图 12-151 所示，在出现的“安装证书”对话框中，选中刚才申请的证书，单击“安装”按钮。

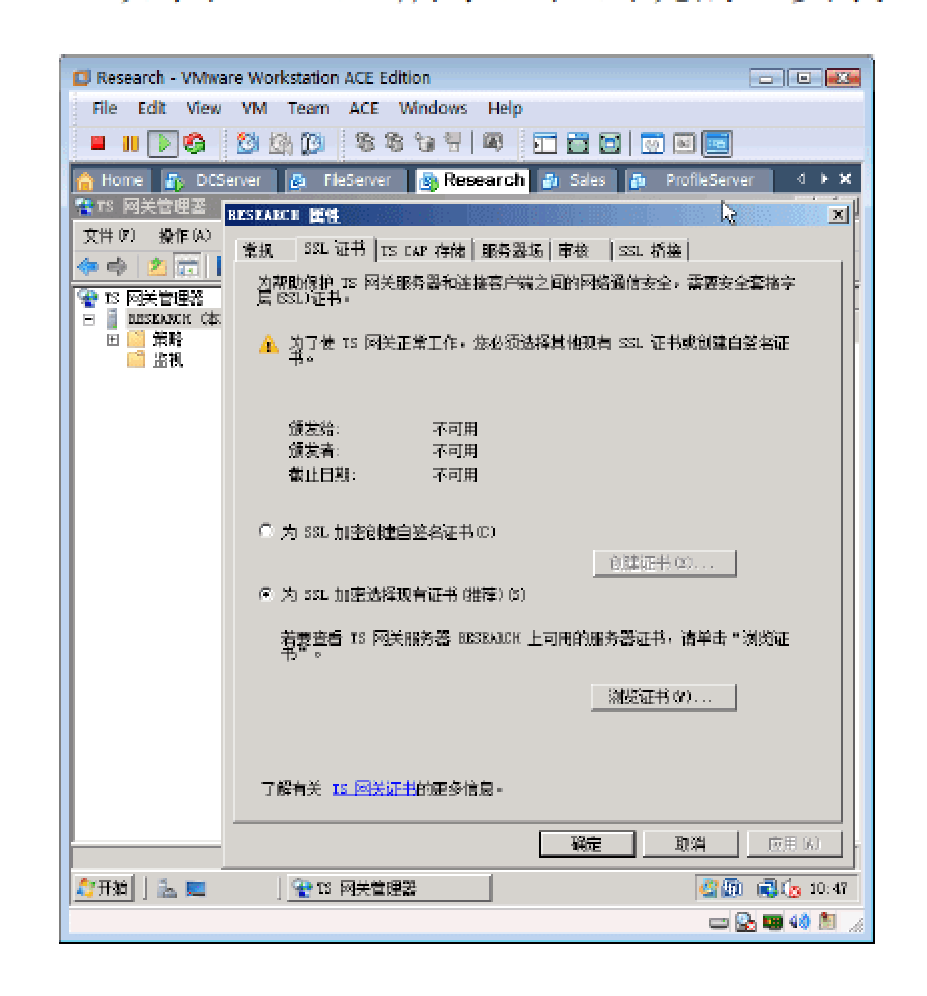


图 12-150　浏览证书

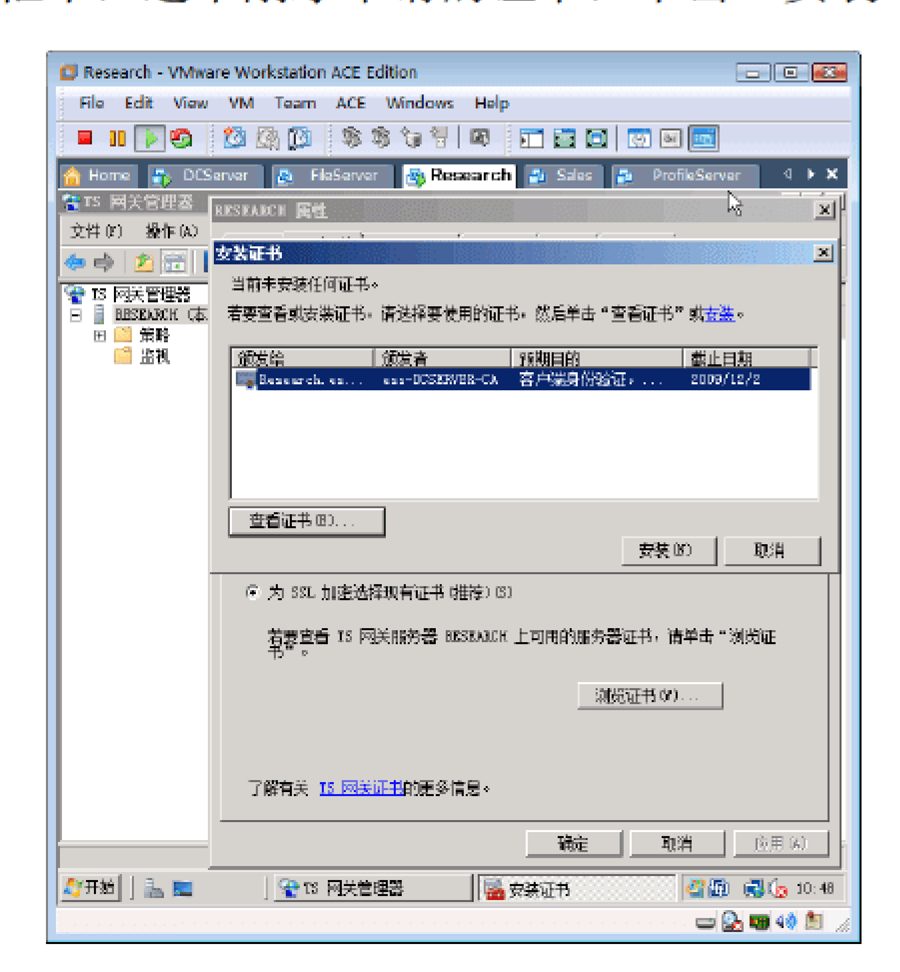


图 12-151　安装证书

12.8.4　任务 4：创建访问策略

1. TS 网关的授权策略

安装了 TS 网关角色服务并为该 TS 网关服务器配置了证书之后，必须创建终端服务连接授权策略（TS CAP）、计算机组和终端服务资源授权策略（TS RAP）。

本主题描述了 TS CAP、计算机组和 TS RAP 如何使你可以控制远程用户通过 TS 网关从 Internet 连接到内部网络时，对内部网络资源(计算机)的访问。

1) TS CAP

通过 TS CAP，可以指定可连接到 TS 网关服务器的用户。可以指定存在于本地 TS 网关服务器上或 Active Directory 域服务中的用户组，还可以指定用户要访问 TS 网关服务器必须满足的其他条件。可以在每个 TS CAP 中列出特定的条件。例如，你可能要求一组用户使用智能卡来通过 TS 网关建立连接。



要点：如果用户满足 TS CAP 中指定的条件，将被授予访问 TS 网关服务器的权限。必须还要创建终端服务资源授权策略（TS RAP）。通过 TS RAP，可以指定用户可通过 TS 网关连接到的网络资源(计算机)。在创建 TS CAP 和 TS RAP 之前，用户无法通过此 TS 网关服务器连接到网络资源。

2) TS RAP

通过 TS RAP，可以指定远程用户可通过 TS 网关服务器连接到的内部网络资源。在创建 TS RAP 时，可以创建计算机组(内部网络上希望远程用户连接到的一组计算机)并将其与 TS RAP 关联。

如果通过 TS 网关服务器连接到内部网络的远程用户至少满足一个 TS CAP 和一个 TS RAP 中指定的条件，将被授予访问网络上的计算机的权限。

注意：将 TS 网关管理的计算机组与 TS RAP 关联时，可以通过将完全限定的域名（FQDN）和 NetBIOS 名称分别添加到受 TS 网关管理的计算机组中，同时支持这两个名称。将 Active Directory 安全组与 TS RAP 关联时，如果客户端要连接到的内部网络计算机与 TS 网关服务器属于同一个域，将自动支持 FQDN 和 NetBIOS 名称；如果内部网络计算机与 TS 网关服务器分别属于不同的域，用户必须指定内部网络计算机的 FQDN。

TS CAP 和 TS RAP 相结合，可提供两个不同的授权级别，使用户可以为内部网络上的计算机配置更具体的访问控制级别。

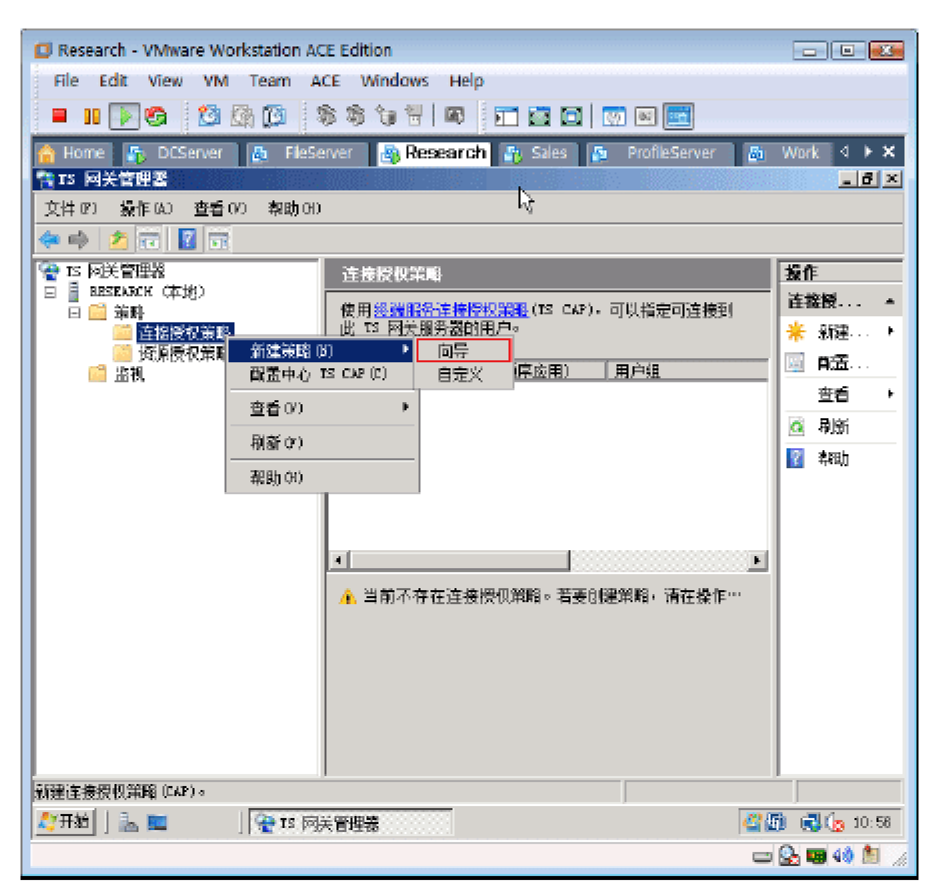
2. 示例

在终端服务网关创建终端服务连接授权策略(TS CAP)、计算机组和终端服务资源授权策略(TS RAP)。

① 以域管理员身份登录到 Research，选择“开始”→“程序”→“管理工具”→“终端服务”→“TS 网关管理器”命令。

② 如图 12-152 所示，右击“连接授权策略”，从弹出的快捷菜单中选择“新建策略”→“向导”命令。

③ 如图 12-153 所示，在出现的“为 TS 网关创建授权策略”界面中，选中“创建 TS CAP 和 TS RAP”单选按钮，单击“下一步”按钮。



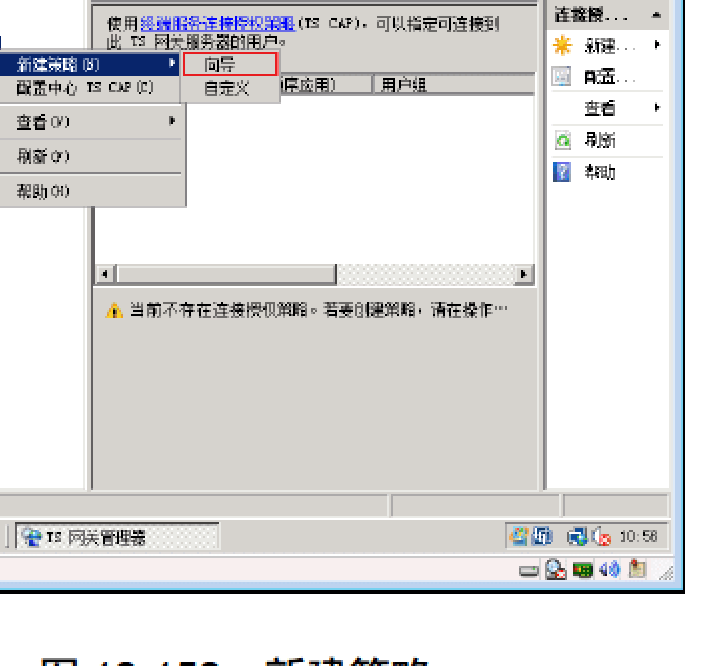


图 12-152　新建策略

图 12-153　创建授权策略

④ 如图 12-154 所示，在出现的“为 TS 网关创建 TS CAP”界面中，输入名称，单击“下一步”按钮。

⑤ 如图 12-155 所示，在出现的对话框中，单击“添加组”按钮，在“用户组成员身份”文本框中输入 ESS\Domain Admins，单击“下一步”按钮。

⑥ 如图 12-156 所示，在出现的“为 TS 网关创建 TS CAP”界面中，选中“启用所有客户端设备的设备重定向”单选按钮，单击“下一步”按钮。

⑦ 如图 12-157 所示，在出现的对话框中，确认设置，单击“下一步”按钮。

⑧ 如图 12-158 所示，在出现的“为 TS 网关创建 TS RAP”界面中，输入授权名称，单击“下一步”按钮。

⑨ 如图 12-159 所示，在出现的对话框中，在“用户组成员身份”文本框中输入 ESS\Domain Admins，

单击“下一步”按钮。

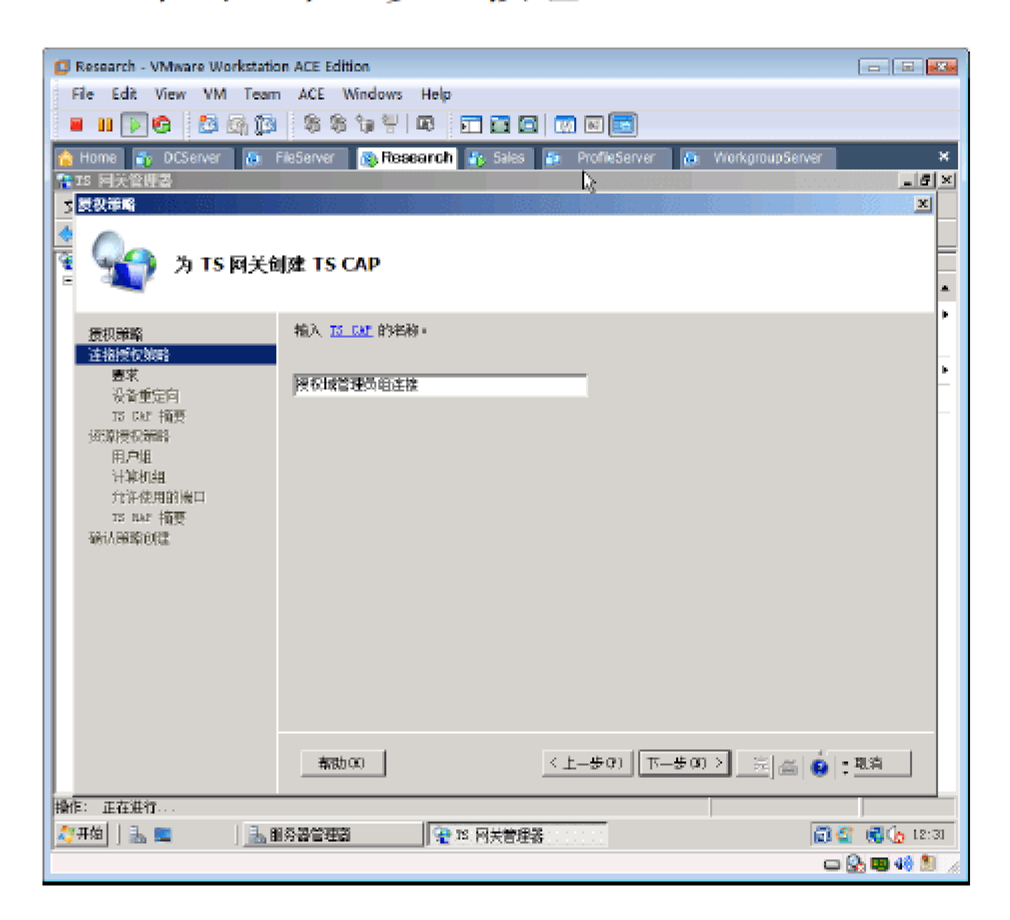


图 12-154 输入名称

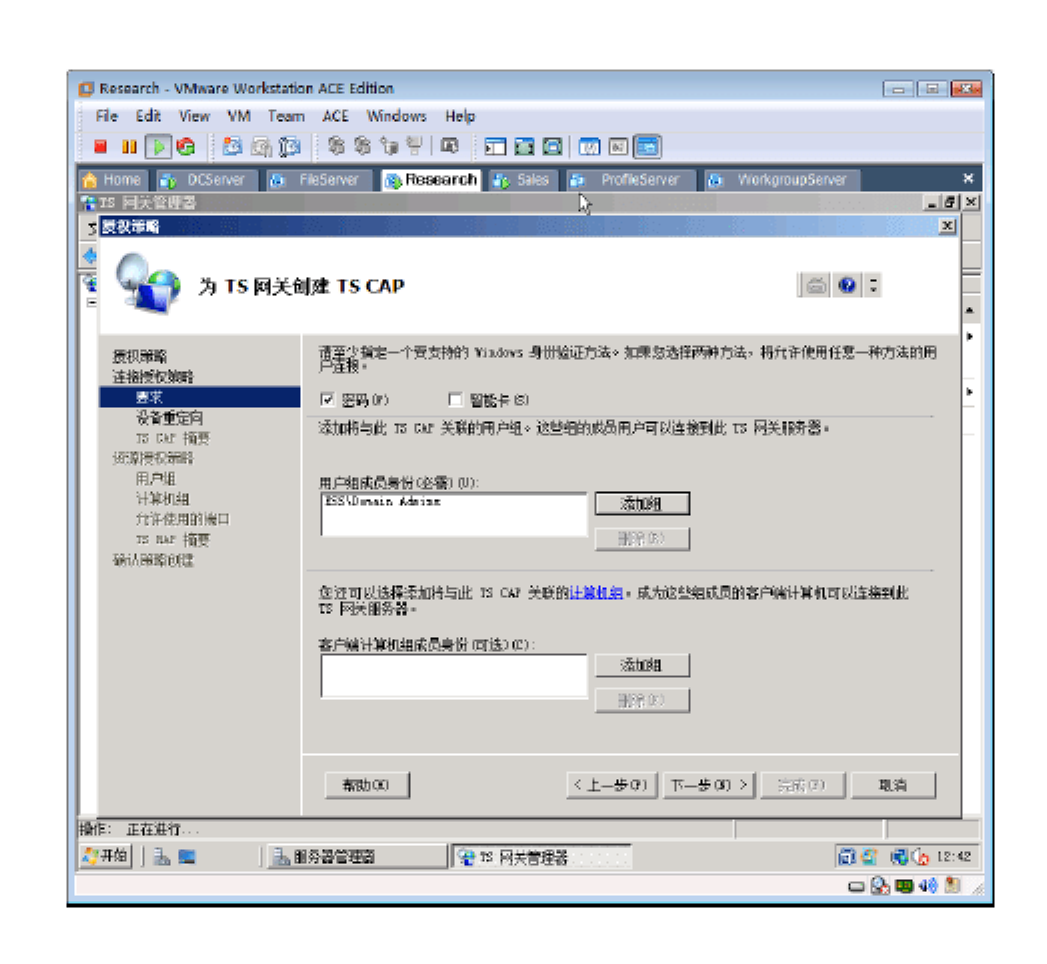


图 12-155 指定成员

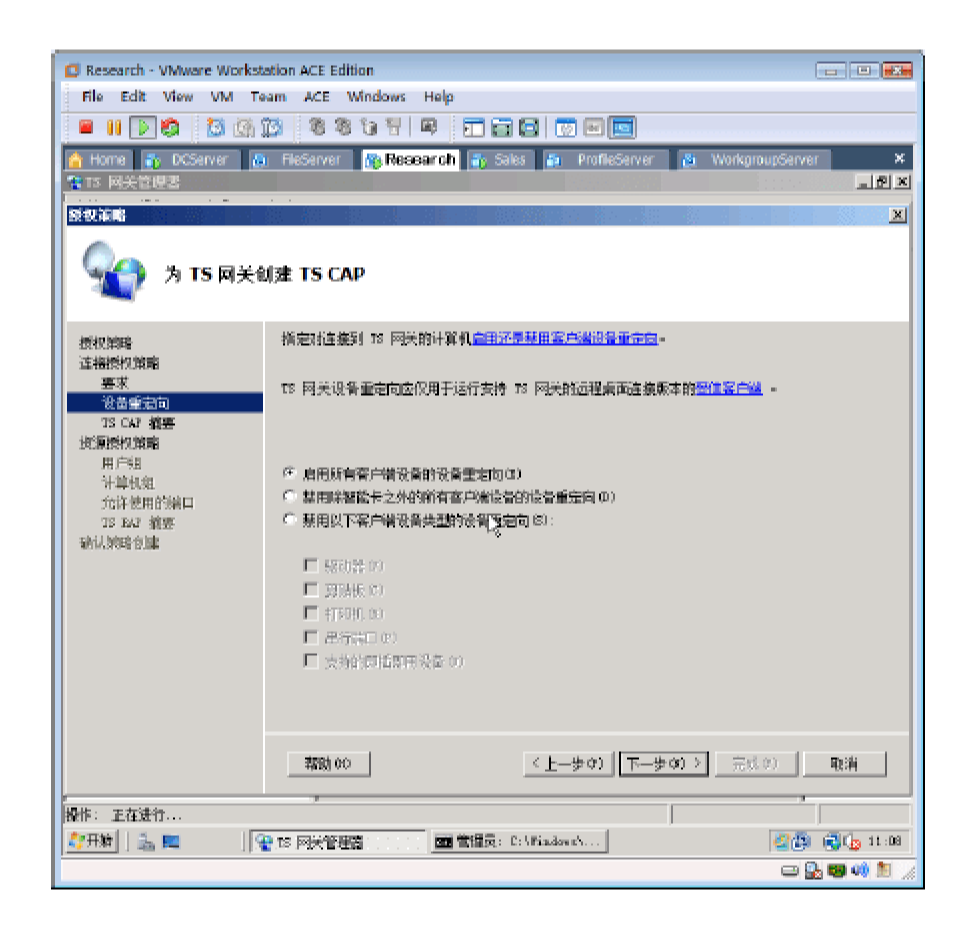


图 12-156 启用设备重定向

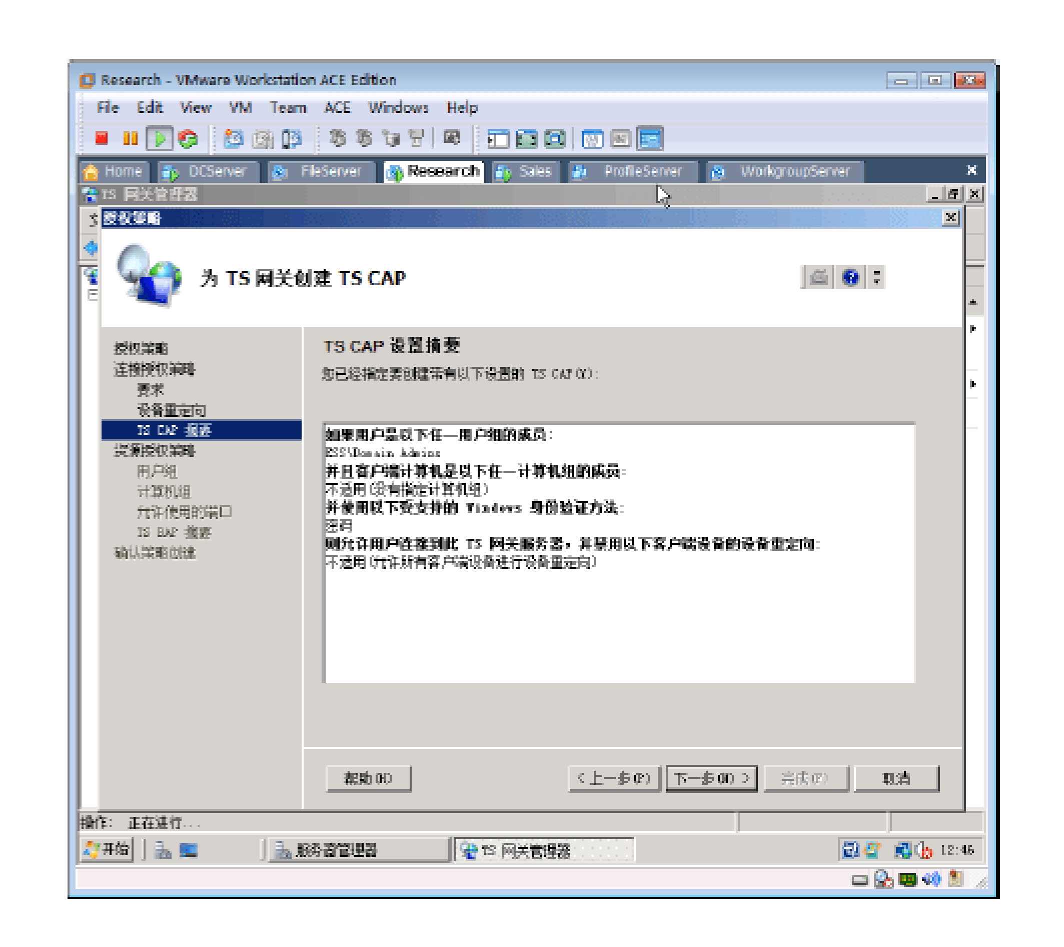


图 12-157 为 TS 网关创建 TS CAP

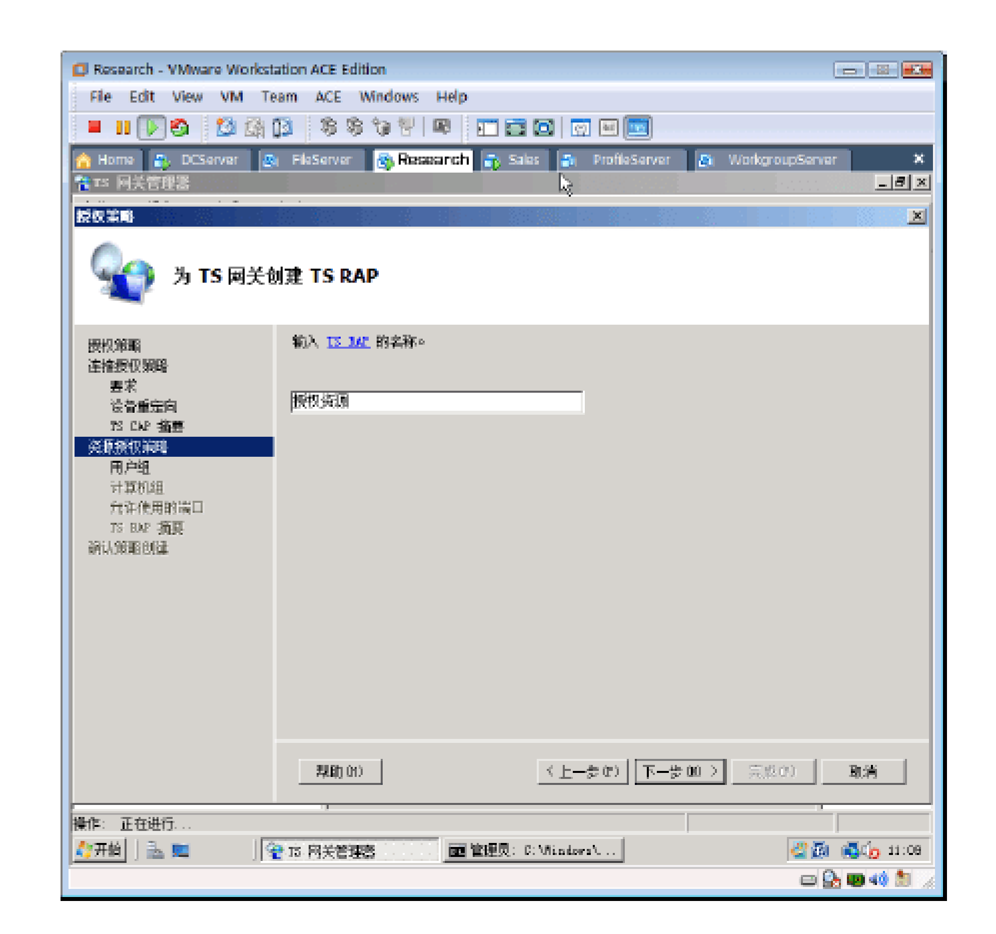


图 12-158 为 TS 网关创建 TS RAP

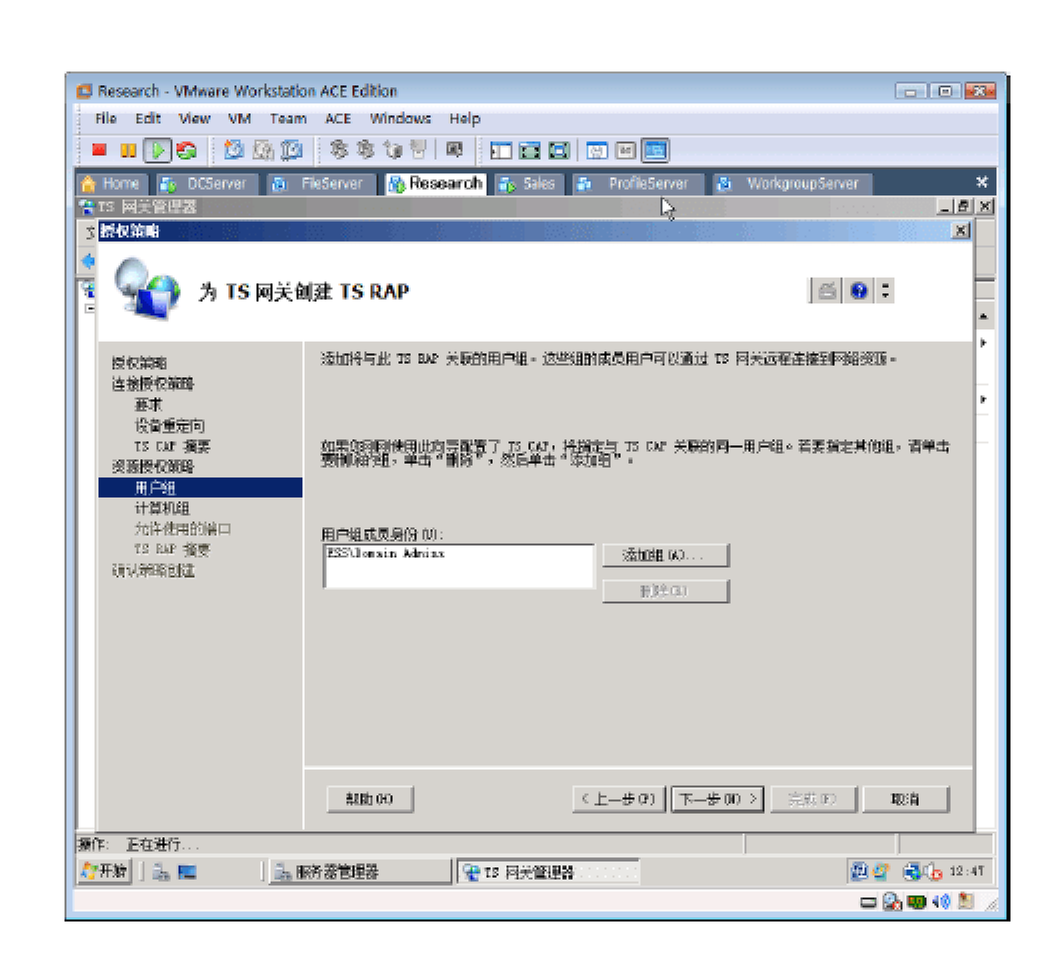


图 12-159 输入用户组

⑩ 如图 12-160 所示，在出现的对话框中，单击“浏览”按钮，在文本框中输入 ESS\Domain Computers，单击“下一步”按钮。

⑪ 如图 12-161 所示，在出现的对话框中，选中“允许通过以下端口连接”单选按钮，在文本框中输入“3389;4000”，单击“下一步”按钮。

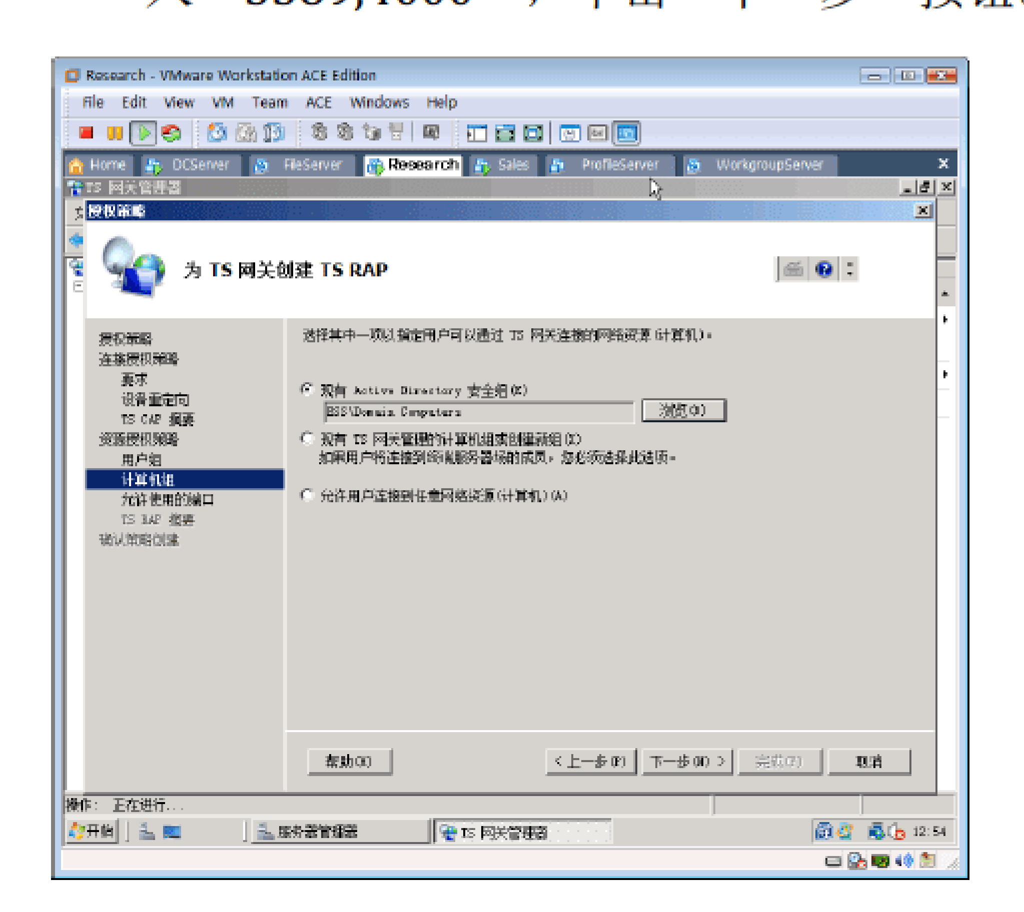


图 12-160　选择终端服务器组

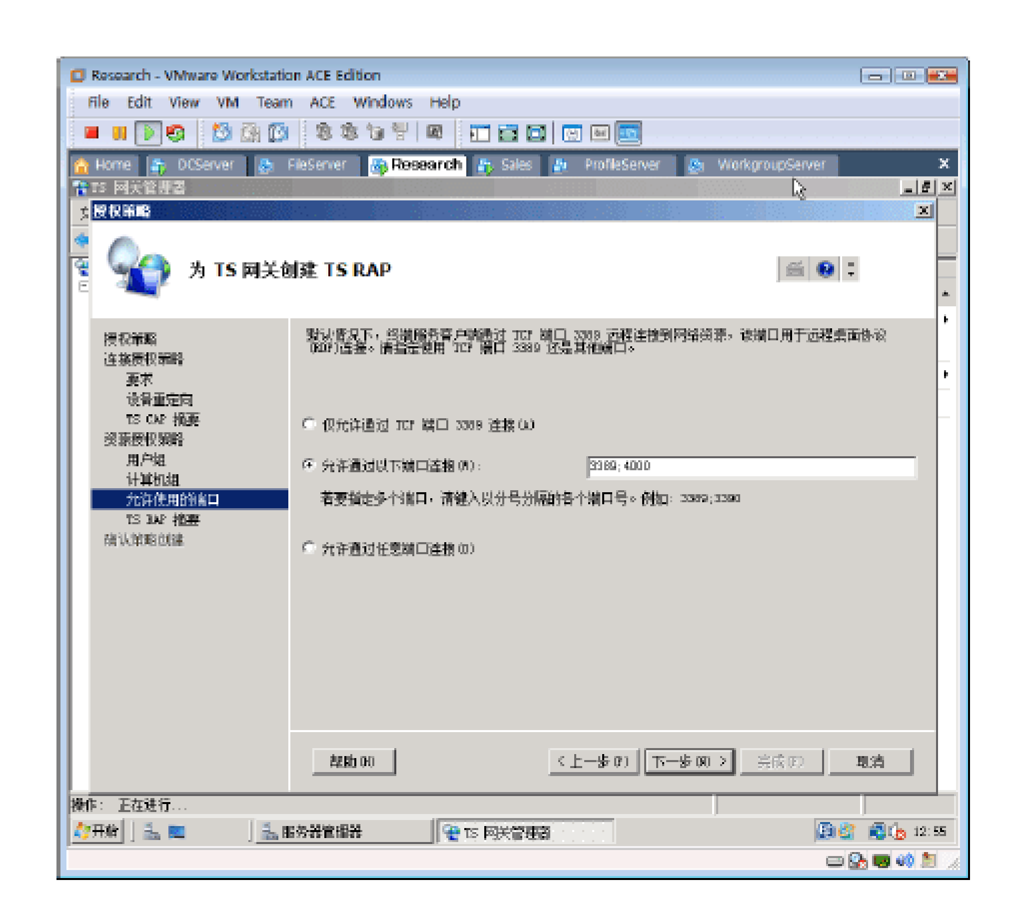


图 12-161　指定端口

⑫ 如图 12-162 所示，在出现的设置摘要对话框中，单击“完成”按钮。

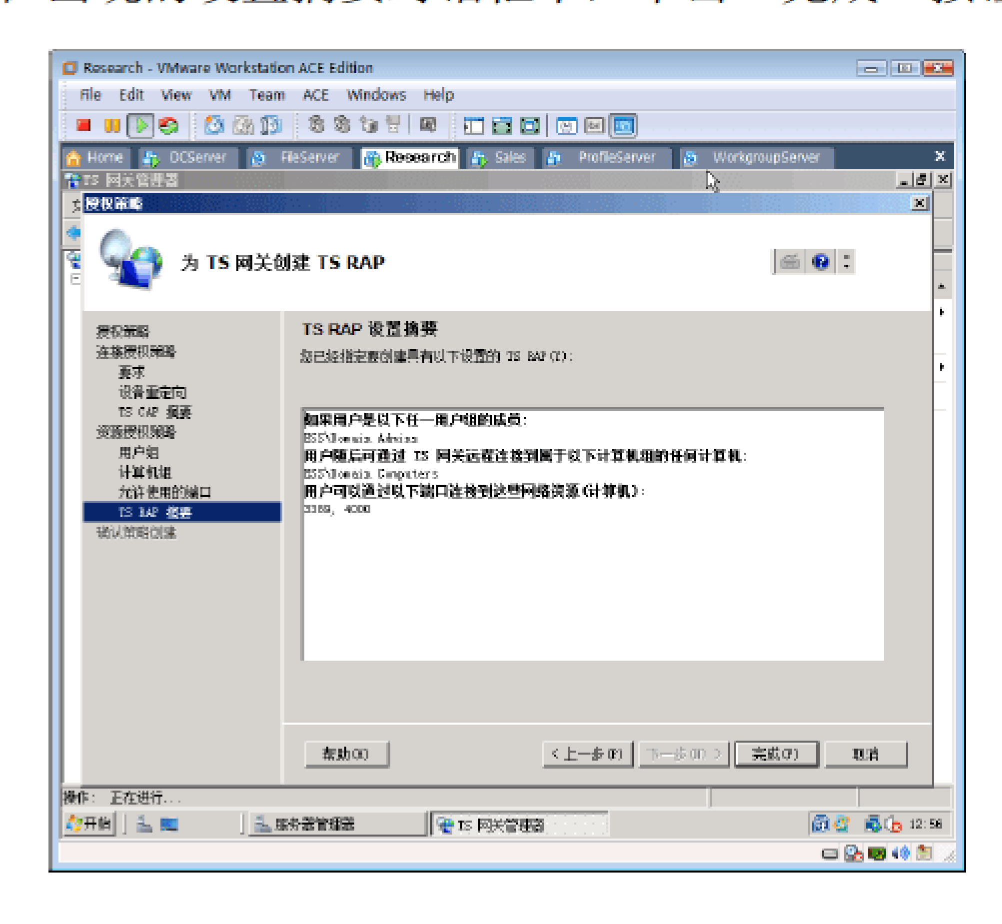


图 12-162　完成 TS 网关创建 TS RAP

12.8.5　任务 5：使用 TS 网关连接到 FileServer

在 WorkgroupServer 上，需要下载企业 CA 的证书。在配置终端服务客户端使用 TS 网关的 Research 服务器连接到企业内部网的终端服务器 FileServer。操作步骤如下。

① 如图 12-163 所示，打开 IE 浏览器，在地址栏中输入 http://dcserver.ess.com/certsrv，在出现的对话框中输入用户名和密码，单击“确定”按钮。

② 如图 12-163 所示，单击“下载 CA 证书、证书链或 CRL”链接。如图 12-164 所示，在出现的 Web 页面上，单击“下载 CA 证书”链接，在弹出的安全警告提示框中单击“保存”按钮。

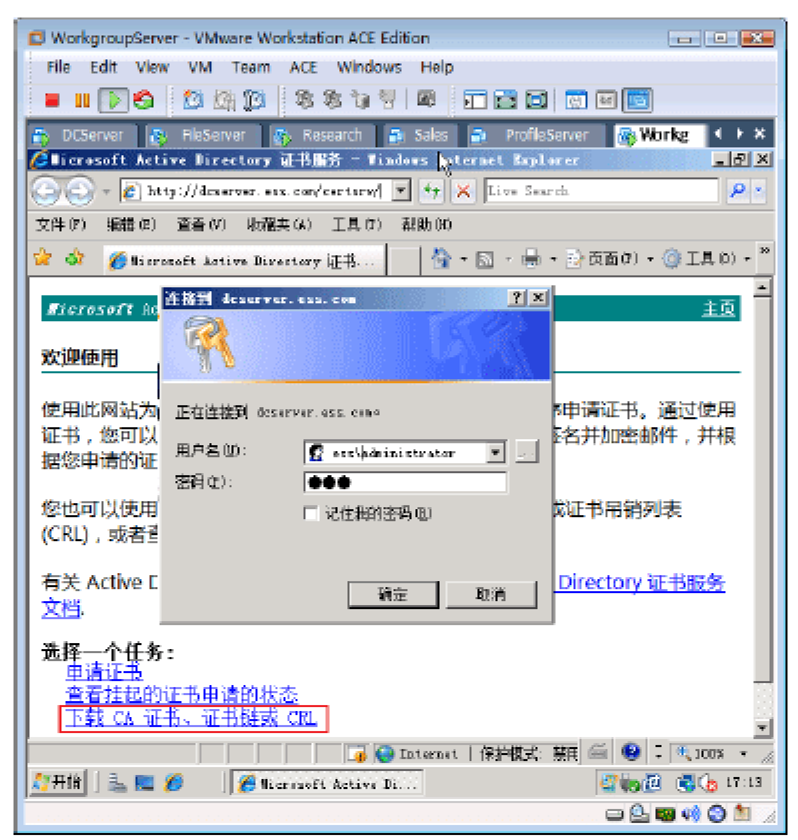
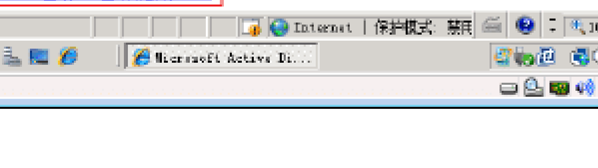



图 12-163　访问 CA Web 站点

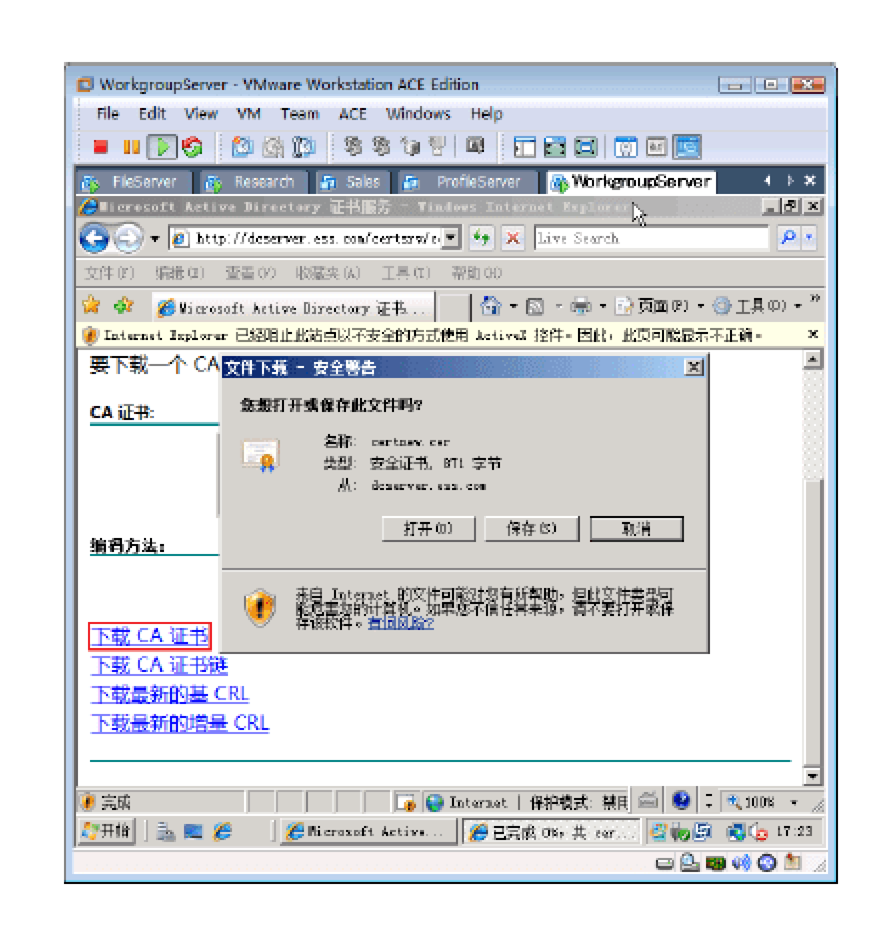


图 12-164　下载 CA 证书

③　如图 12-165 所示，右击桌面上的 IE 浏览器，在弹出的快捷菜单中选择“属性”命令，在“Internet 属性”对话框的“内容”选项卡中，单击“证书”按钮。

④　如图 12-166 所示，在“证书”对话框的“受信任的根证书颁发机构”选项卡中，单击“导入”按钮，将刚才下载的 CA 证书导入。

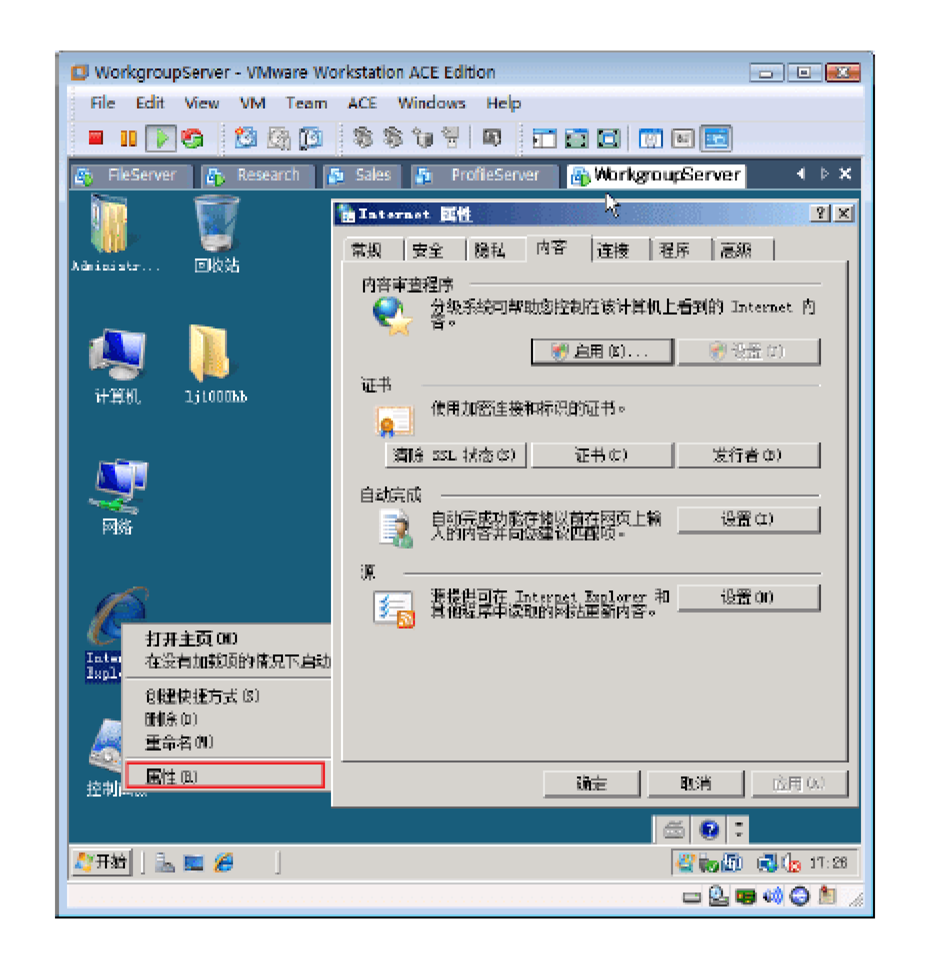


图 12-165　打开 IE 属性

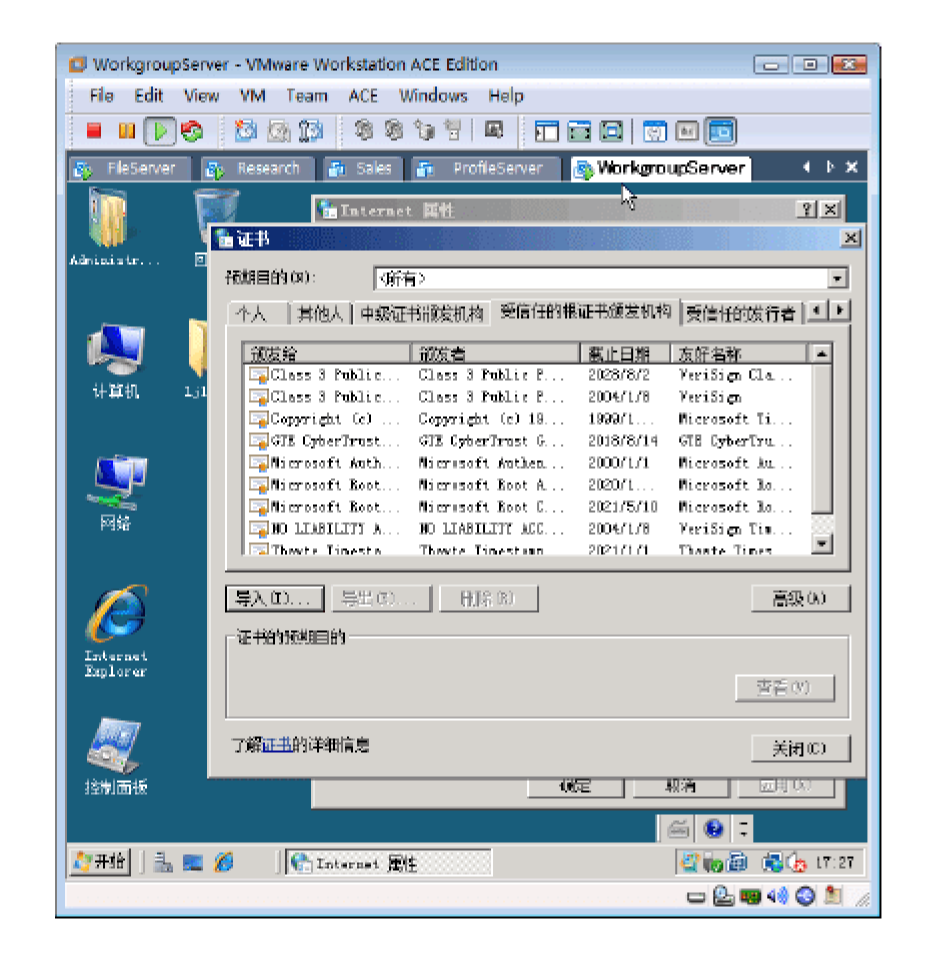


图 12-166　受信任的证书颁发机构

⑤　如图 12-167 所示，在出现的“安全性警告”对话框中，单击“是”按钮，完成导入。这样当前用户就信任该证书颁发机构了。

⑥　如图 12-168 所示，选择“开始”→“运行”命令，在出现的“运行”对话框中输入 mstsc，打开终端服务客户端，单击“选项”按钮，在“计算机”下拉列表框中输入 fileServer.ess.com。

⑦　如图 12-169 所示，在“高级”选项卡中，单击“设置”按钮。

⑧　如图 12-170 所示，在“TS 网关服务器设置”对话框中，选中“使用这些 TS 网关服务器设置”单选按钮，输入 TS 网关服务器名称，选中“将我的 TS 网关凭据用于远程计算机”复选框，单击“确定”按钮。这里一定要使用计算机域名访问 TS。

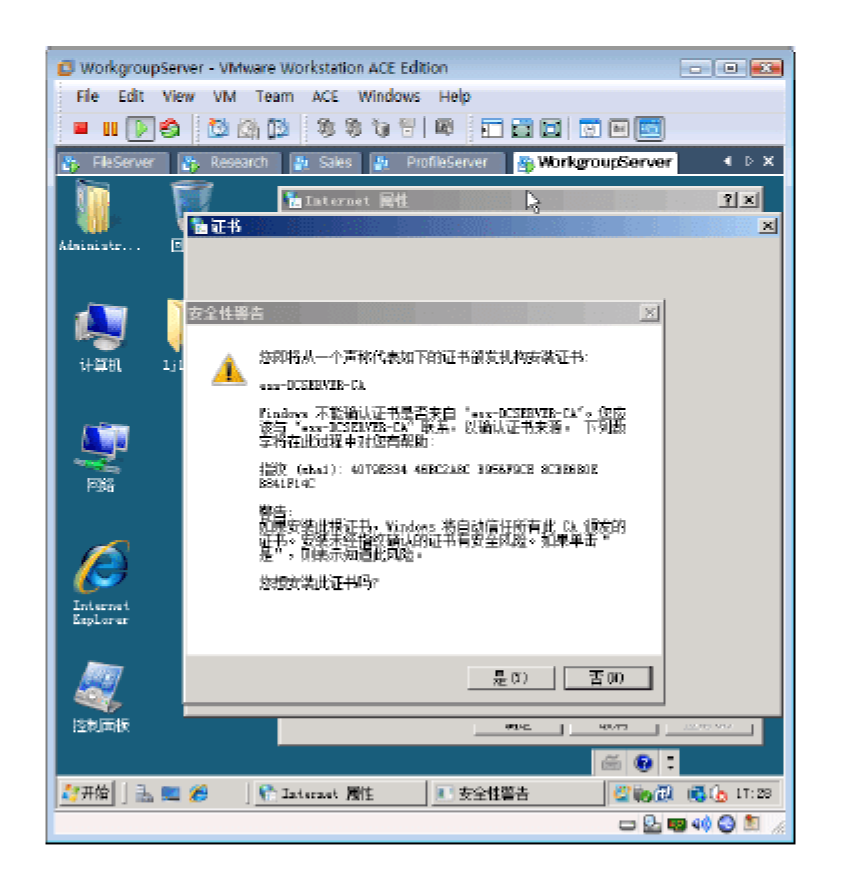


图 12-167　提示框

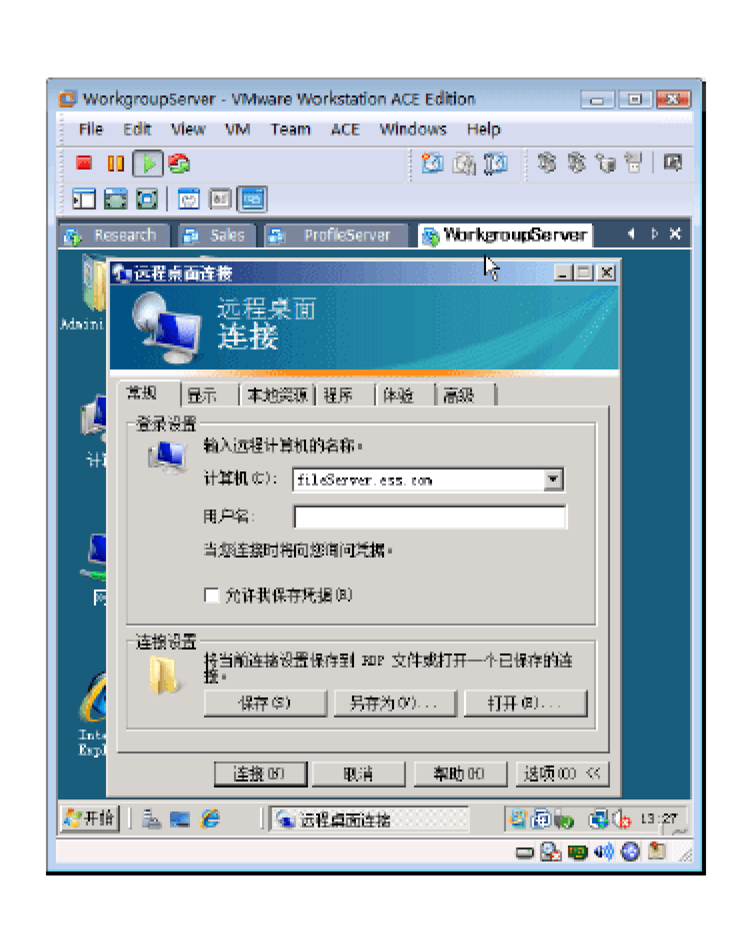


图 12-168　连接服务器

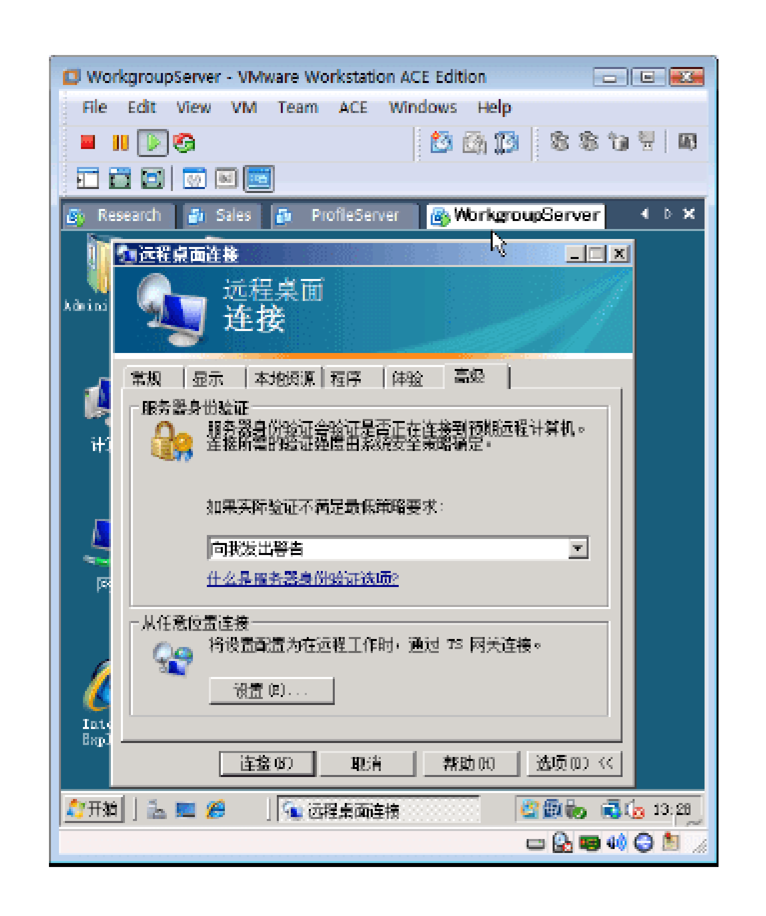


图 12-169　配置 TS 网关

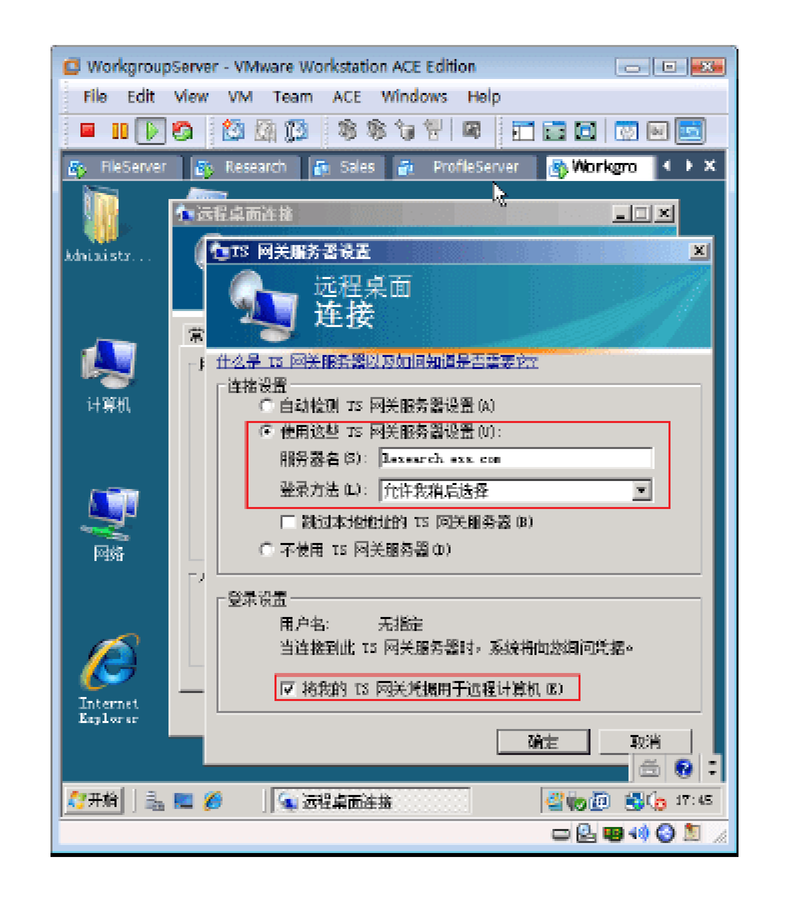


图 12-170　指定 TS 网关

⑨　如图 12-171 所示，在出现的“Windows 安全”对话框中，输入域管理员账号和密码，单击“确定”按钮。

⑩　如图 12-172 所示，可以看到能够使用终端服务网关 Research 连接到终端服务器 FileServer。

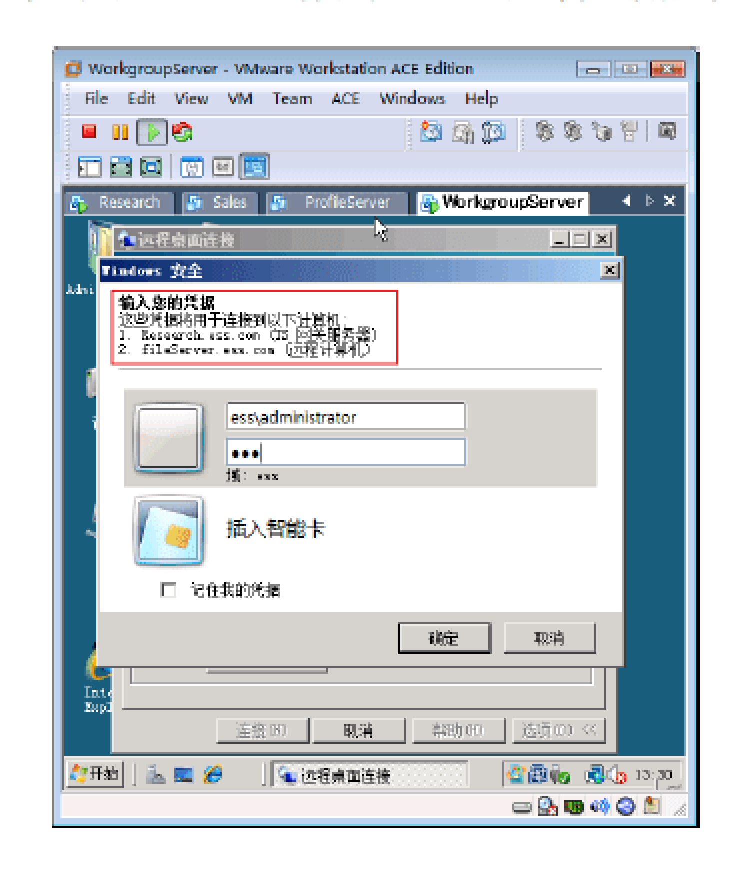


图 12-171　输入账号和密码

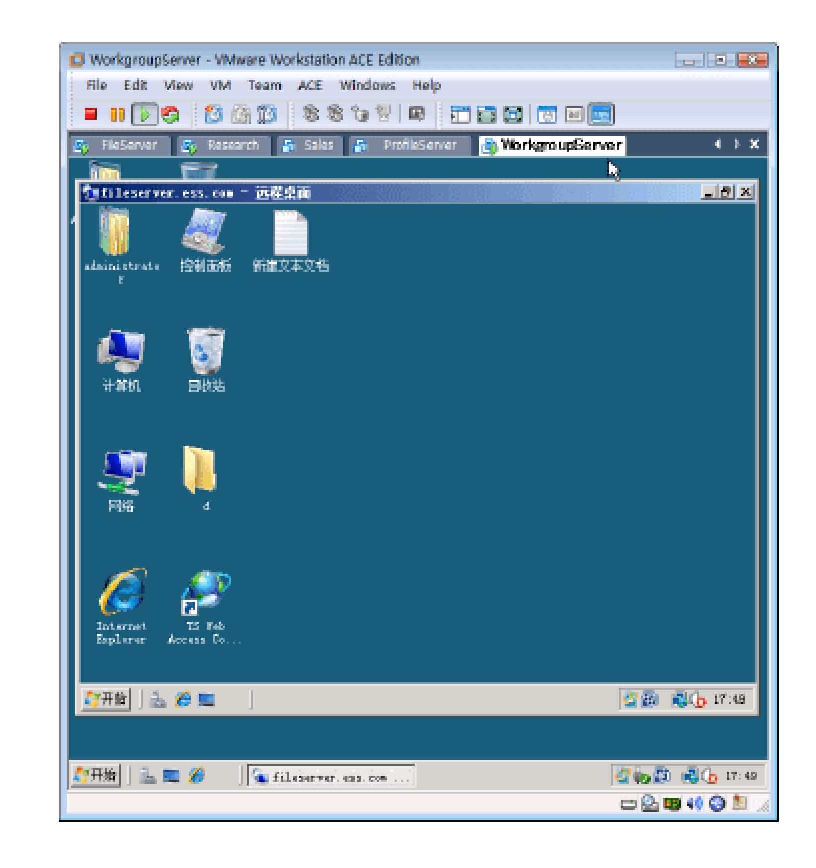
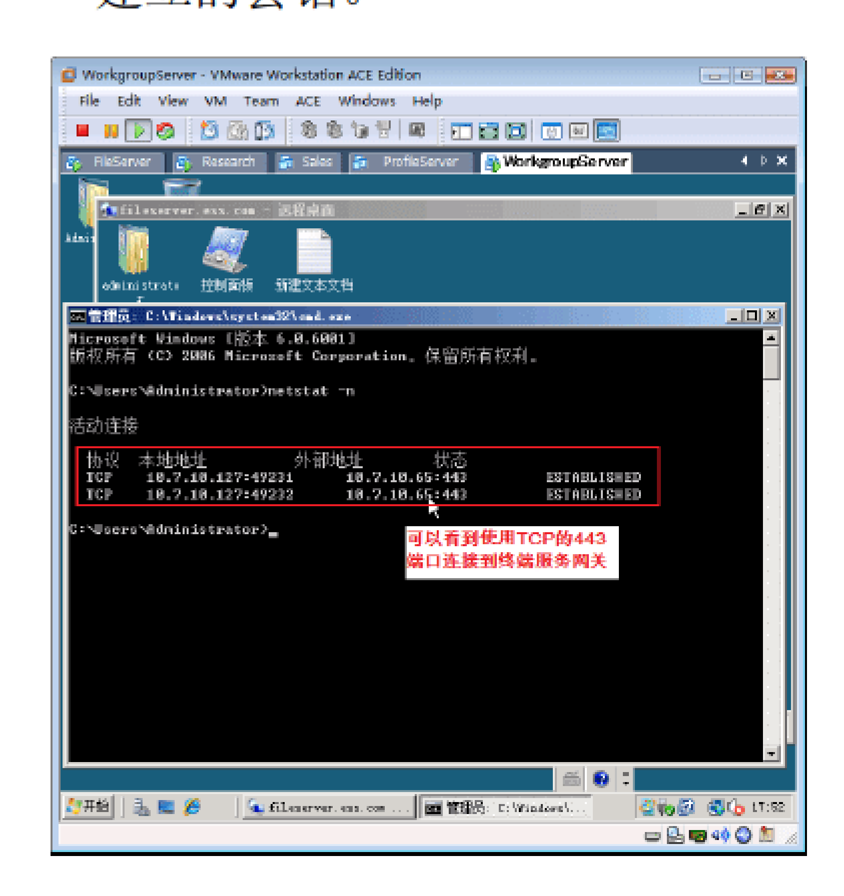


图 12-172　使用 TS 网关连接内网服务器

⑪　如图 12-173 所示，在命令行状态下输入 netstat –n，可以看到与终端服务网关建立的会话使用的是 TCP 的 443 端口。

⑫　如图 12-174 所示，在 FileServer 上可以看到终端服务器是使用 TCP 的 3389 端口与终端服务网关建立的会话。





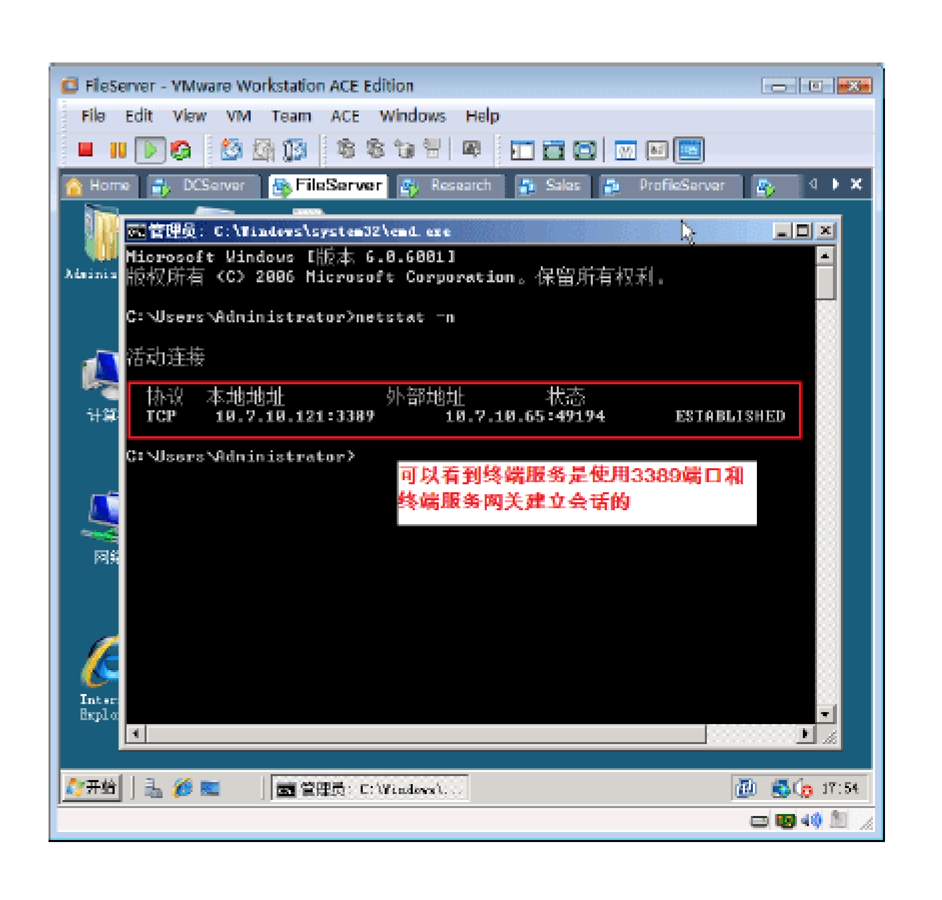
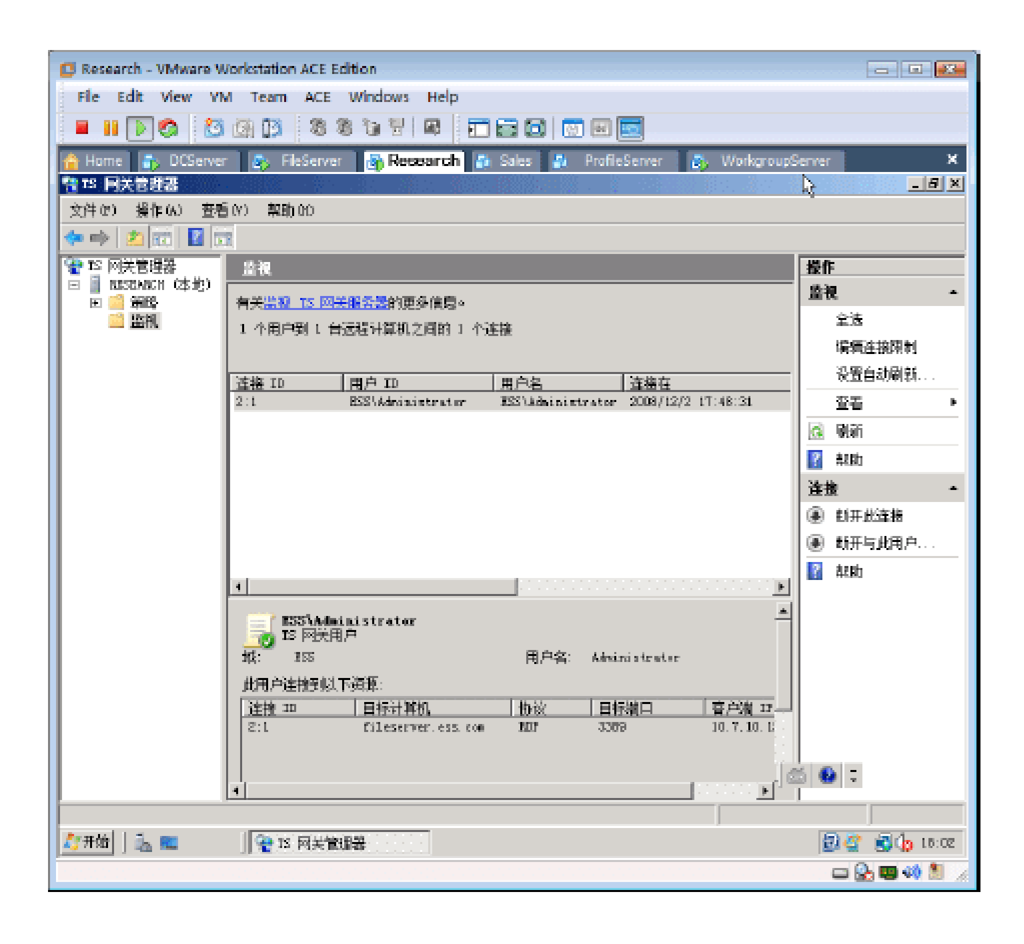


图 12-173　查看会话　　　　图 12-174　在终端服务器上查看会话

⑬　如图 12-175 所示，在终端服务器网关 Research 计算机上，打开 TS 网关管理器，单击“监视”选项，可以看到连接到内网的终端服务会话。



> **提示：** 如图 12-176 所示，使用 TS 网关访问 dcserver.ess.com，提示不满足资源访问策略，因为资源访问策略只允许访问 Domain Computers，而域控制器不属于这个组。



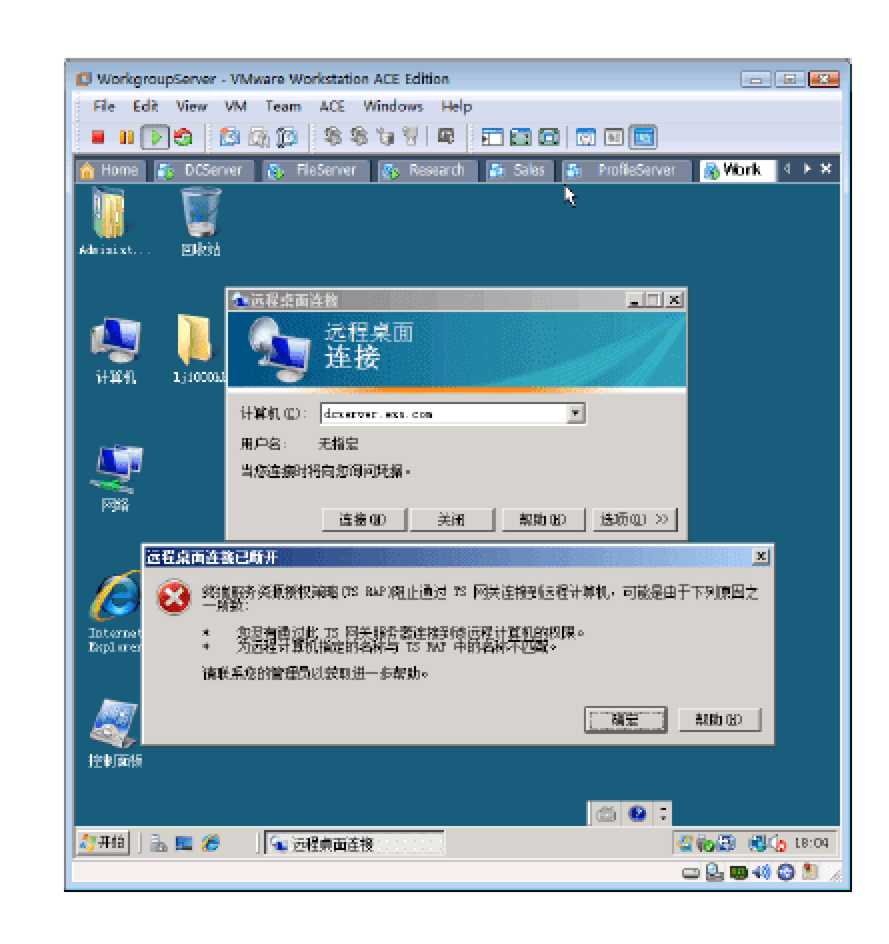


图 12-175　在 TS 网关上查看会话　　　　图 12-176　不满足资源访问策略

12.8.6　任务 6：使用 TS 网关连接到 Windows Server Core 远程桌面

①　在 WorkgroupServer 上打开终端服务客户端，如图 12-177 所示，配置使用终端服务网关，输入 profileServer.ess.com，单击“连接”按钮，在出现的对话框中输入域管理员账号和密码，单击“确

定”按钮。

② 如图 12-178 所示，出现 Windows Server Core 的桌面，输入 Logoff，注销。

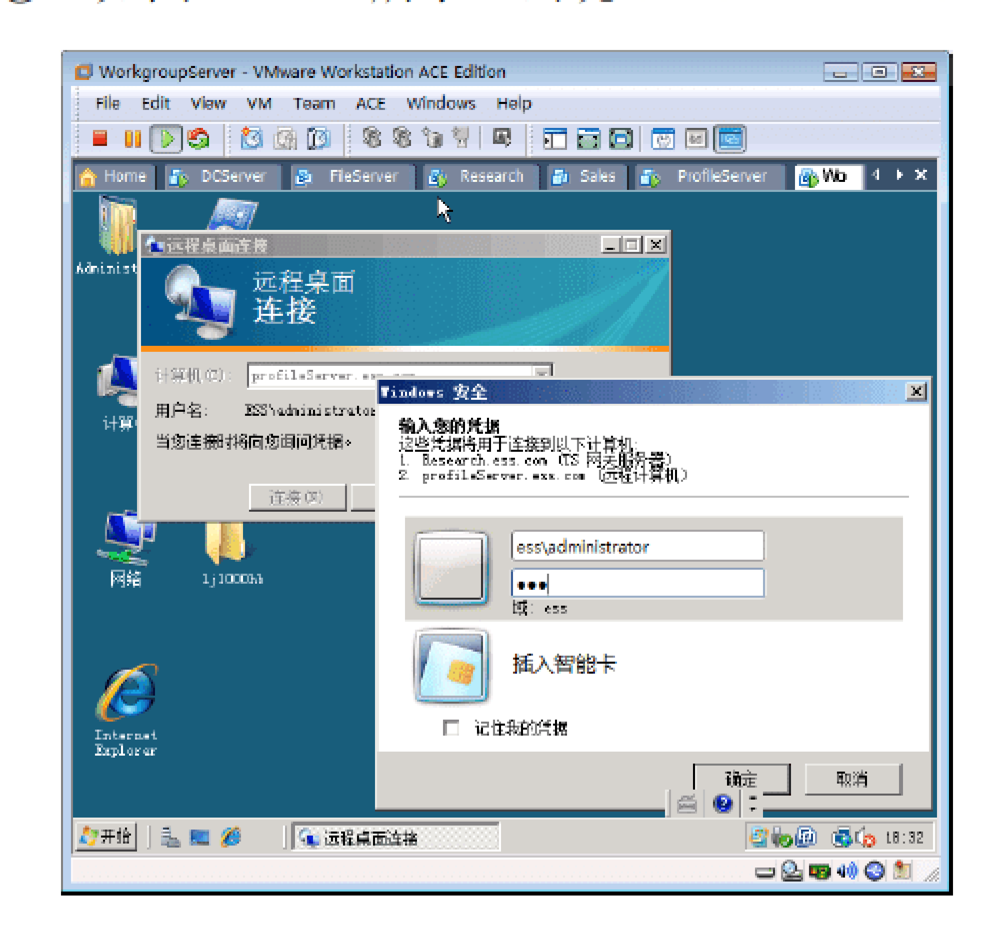


图 12-177　连接到内网的 Server Core

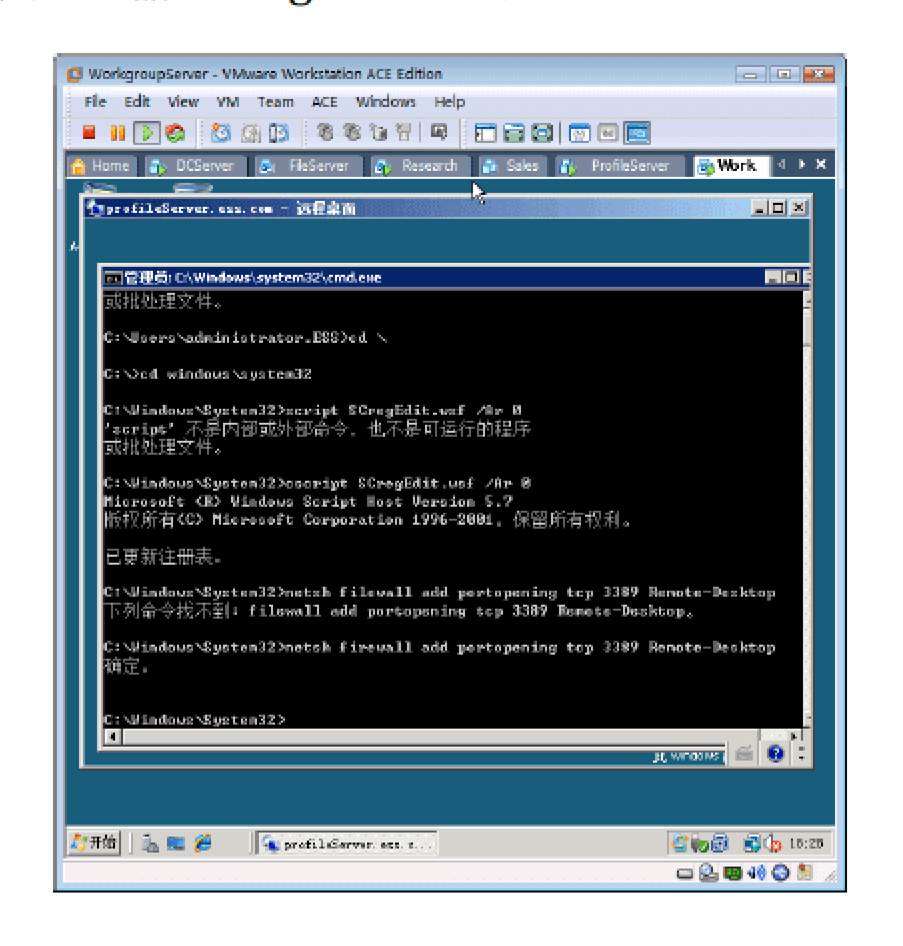


图 12-178　登录成功

12.9　TS Session Broker

TS Session Broker 是 Windows Server 2008 中的新特点，是用于终端服务的 Microsoft Network Load Balancing 更简单的一个替代产品。该特点并不局限于某些服务器，而是为 2～5 台服务器中心提供了极大价值。通过 TS Session Broker，新会话分布在整个中心任务最少的服务器上，这不但可以优化性能，同时允许用户与现有会话重新连接，而无须知道关于服务器建立地点的具体信息。IT 经理可以利用这一特点为单一域名系统(DNS)入口绘制每个终端服务器的 IP 地址地图。这一配置提供故障误差，一旦中心服务器不可使用，用户可以连接到中心里工作量为倒数第二的服务器。

TS Session Broker 可提供下列功能的角色服务。

- 使用户可以重新连接到负载平衡终端服务器场中的现有会话。
- 使用户可以将会话负载在负载平衡终端服务器场中的服务器之间均匀分配。

TS Session Broker 存储会话状态信息，包括会话 ID、会话关联的用户名以及每个会话所在的服务器的名称。

如果用户与会话断开(无论是有意断开还是由于网络故障而断开)，其应用程序仍将继续运行。在重新连接时，将查询 TS Session Broker，以确定是否有现有会话，如果有，则确定会话在场中的哪台服务器上。如果有现有会话，TS Session Broker 会将客户端重定向到其会话所在的终端服务器。

通过 TS Session Broker 负载平衡，没有现有会话的用户连接到负载平衡的场中的终端服务器时，会将用户重定向到会话数最少的终端服务器。(若要在场中比较强大和不太强大的服务器之间分配会话负载，可以为服务器分配相对服务器权重值)如果有现有会话的用户重新连接，则将用户重定向到其现有会话所在的终端服务器。

TS Session Broker 组件

TS Session Broker 服务器是运行 Terminal Services Session Broker 服务并跟踪一个或多个负载平衡终

端服务器场的用户会话的服务器。TS Session Broker 使用场名称确定处于同一个终端服务器场中的服务器。

使用 TS Session Broker 的终端服务器，是作为 TS Session Broker 中的场的成员的负载平衡终端服务器。

若要参与 TS Session Broker，服务器必须符合下列条件。

- 服务器必须安装了“终端服务器”角色服务。
- 服务器必须是 Active Directory 域的成员。
- 服务器必须是负载平衡终端服务器场的成员。

> **注意**：如果要使用 TS Session Broker 负载平衡功能，可以将负载平衡设置与其他 TS Session Broker 设置一起进行配置。如果使用 TS Session Broker 负载平衡，场中的所有终端服务器必须均在运行 Windows Server 2008。

- 服务器必须是 TS Session Broker 服务器上的 Session Directory Computers 本地组的成员。
- 服务器必须加入 TS Session Broker 中的场。

> **要点**：如果终端服务器运行的是某个版本的 Windows Server 2008，则只能使用同样运行某个版本的 Windows Server 2008 的 TS Session Broker 服务器。

实验环境

如图 12-179 所示为某钢厂正在测试开发的财务软件。为了更改和部署程序方便，将测试阶段的程序安装在两个终端服务器 Research 和 FileServer 上，但数据库使用的是同一个服务器上的 SQL Server 上的数据库。财务人员使用终端服务客户端连接到这两个终端服务，为了实现负载均衡，在 DCServer 上安装 TS Session Broker。

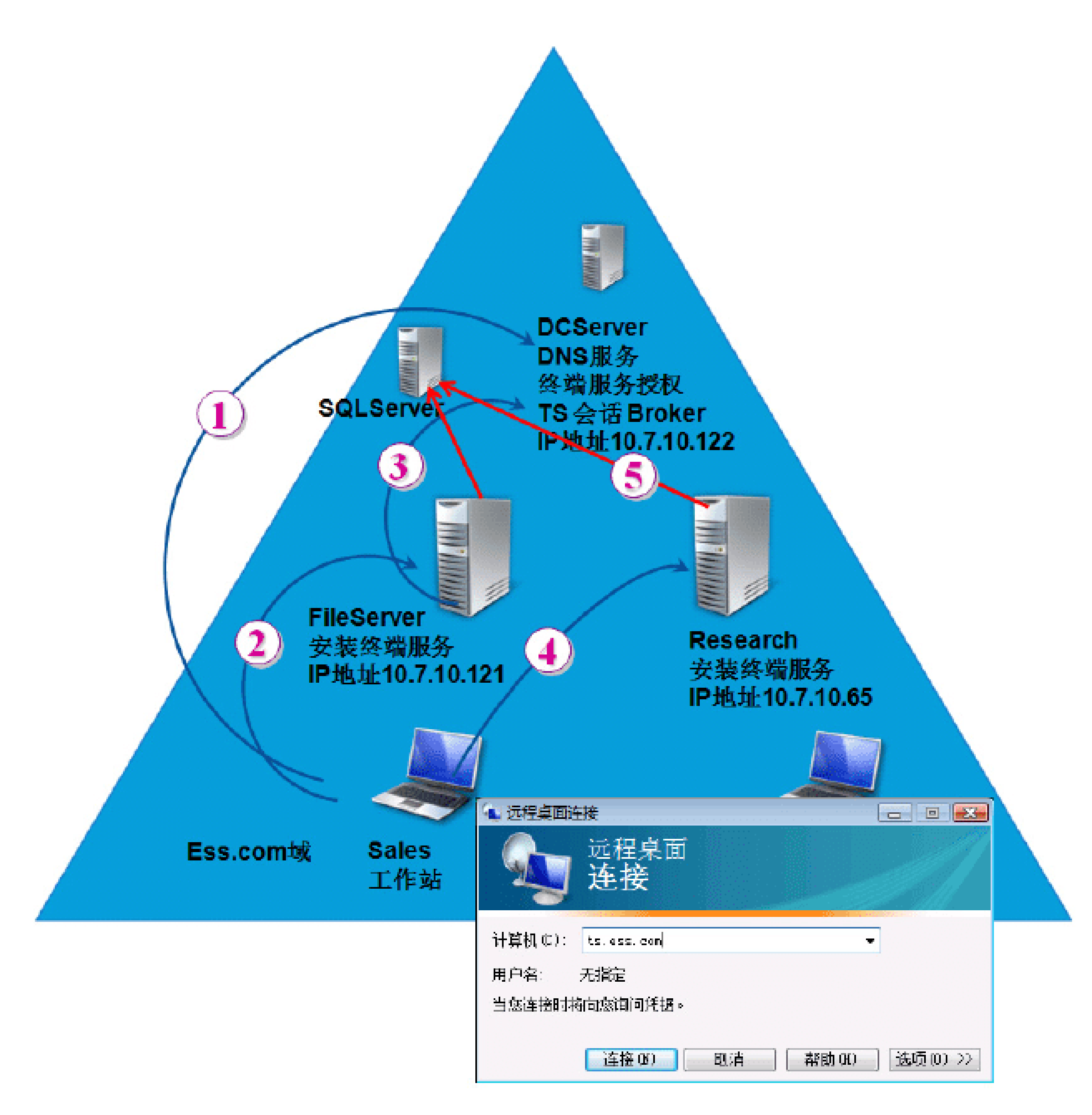


图 12-179　实验环境

操作系统

- DCServer 是 Ess.com 域中的域控制器，安装 Windows Server 2008 企业版操作系统，安装有 TS 会话 Broker、DNS 服务器和终端服务授权。
- FileServer 和 Research 是 Ess.com 域中的应用程序服务器，Windows Server 2008 企业版操作系统，安装终端服务和财务软件。
- Sales 计算机是 Ess.com 域中的计算机，是财务人员的工作站。

要求

- 财务人员使用远程桌面连接 ts.ess.com 连接到这两个终端服务器。
- 将财务人员的终端服务会话分摊到 FileServer 和 Research 服务器。

TS 会话 Broker 的工作步骤如下。

① Sales 计算机的远程桌面连接，输入 ts.ess.com。通过 DNS 解析到 ts.ess.com 域名两个 IP 地址，10.7.10.121 和 10.7.10.65。

② Sales 计算机连接第一个地址 10.7.10.121。

③ 终端服务器 FileServer 查找 TS 会话 Broker。

④ 由 TS 会话 Broker 根据终端服务负载将用户指定到终端会话较少的服务器，如果是断开的终端服务会话连接过来，会将用户定位到原来使用的终端服务器上。

⑤ 客户无论使用哪个终端服务器上的程序，都是连接的同一个 SQL Server 数据库服务器上的数据库。

这样对于使用者，不必关心连接的是哪个终端服务器，结果都是相同程序、相同的数据。如果终端服务器上的用户访问的数据存储在本地文件夹，为了让用户连接到不同终端服务器都能看到相同文件夹，可以使用 DFS 将终端服务器上的文件夹进行数据实时同步。

以下任务将会演示在域环境中配置使用 TS 会话 Broker 实现终端服务的负载均衡。

12.9.1 任务 1：在 DCServer 中安装 TS 会话 Broker

① 以域管理员账户登录到 DCServer，打开服务器管理器，如图 12-180 所示，单击“添加角色服务”按钮。

② 如图 12-181 所示，选中“TS 会话 Broker”复选框，单击“下一步”按钮，完成安装。

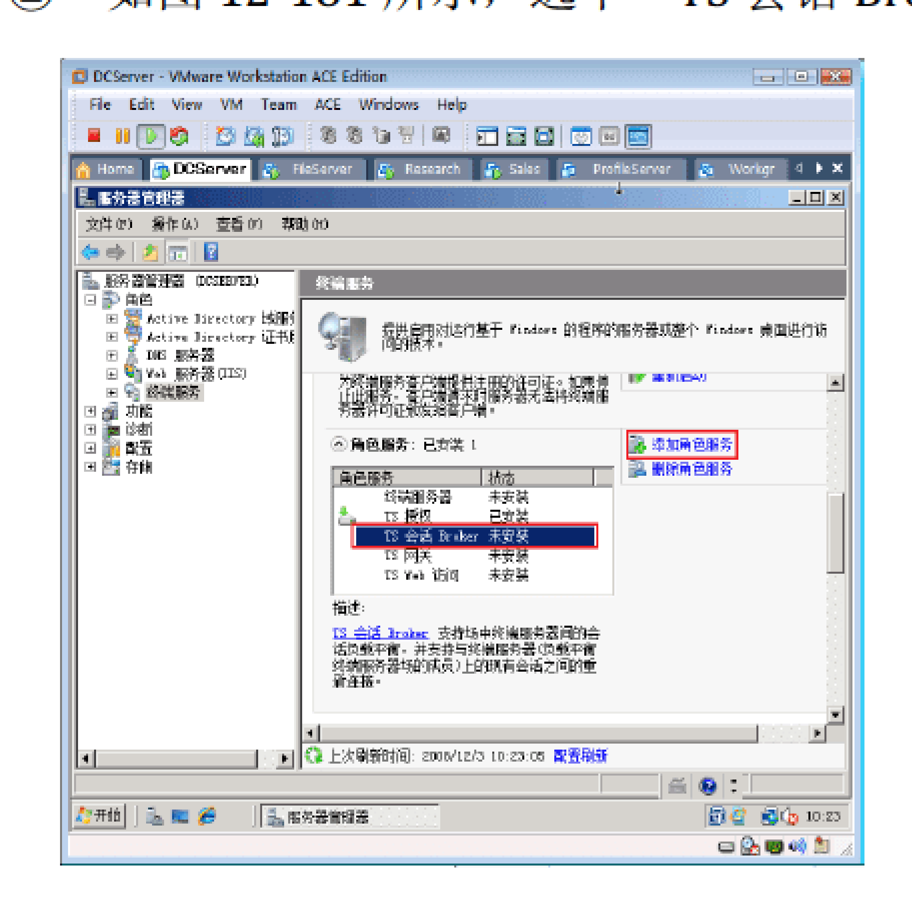


图 12-180 添加角色服务

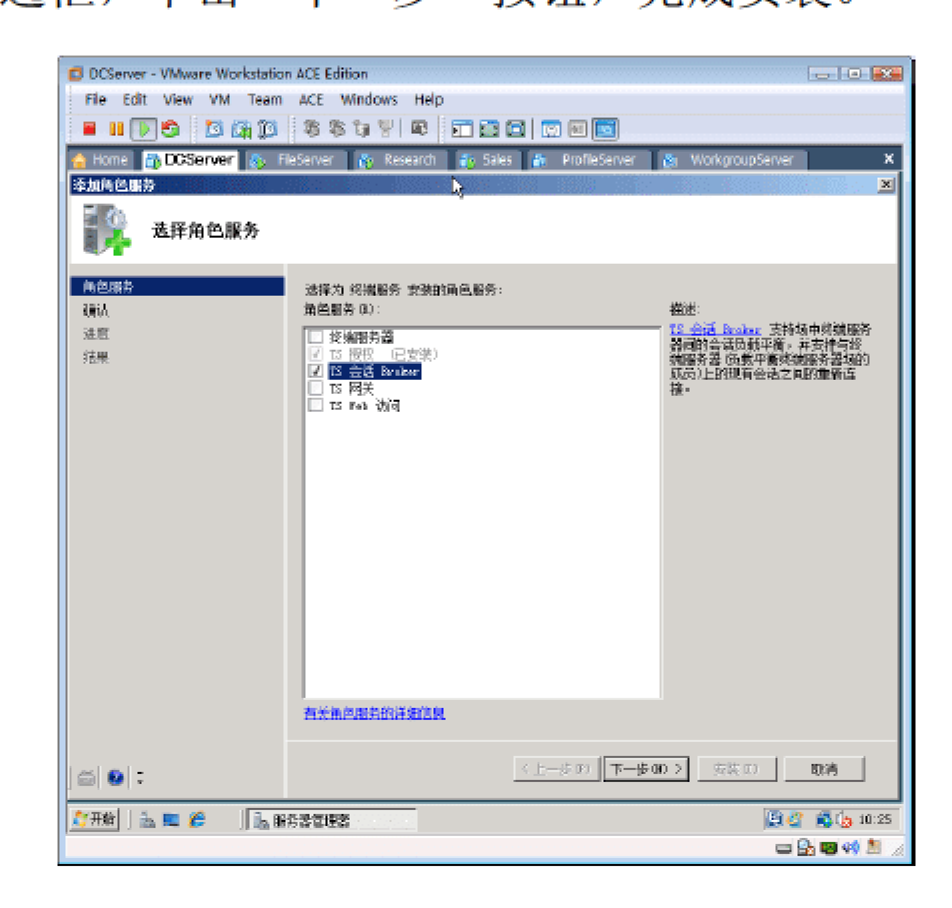


图 12-181 选择角色服务

③ 选择“开始”→“运行”命令，在出现的“运行”对话框中输入 dsa.msc，单击“确定”按钮，打开“Active Directory 用户和计算机”管理工具。

④ 如图 12-182 所示，双击 Session Directory Computers 组，在出现的对话框的“成员”选项卡中，单击“添加”按钮。

⑤ 如图 12-183 所示，在出现的“添加用户、联系人、计算机或组”对话框中，单击“对象类型”按钮。

⑥ 如图 12-183 所示，在出现的“对象类型”对话框中，选中“计算机”复选框。

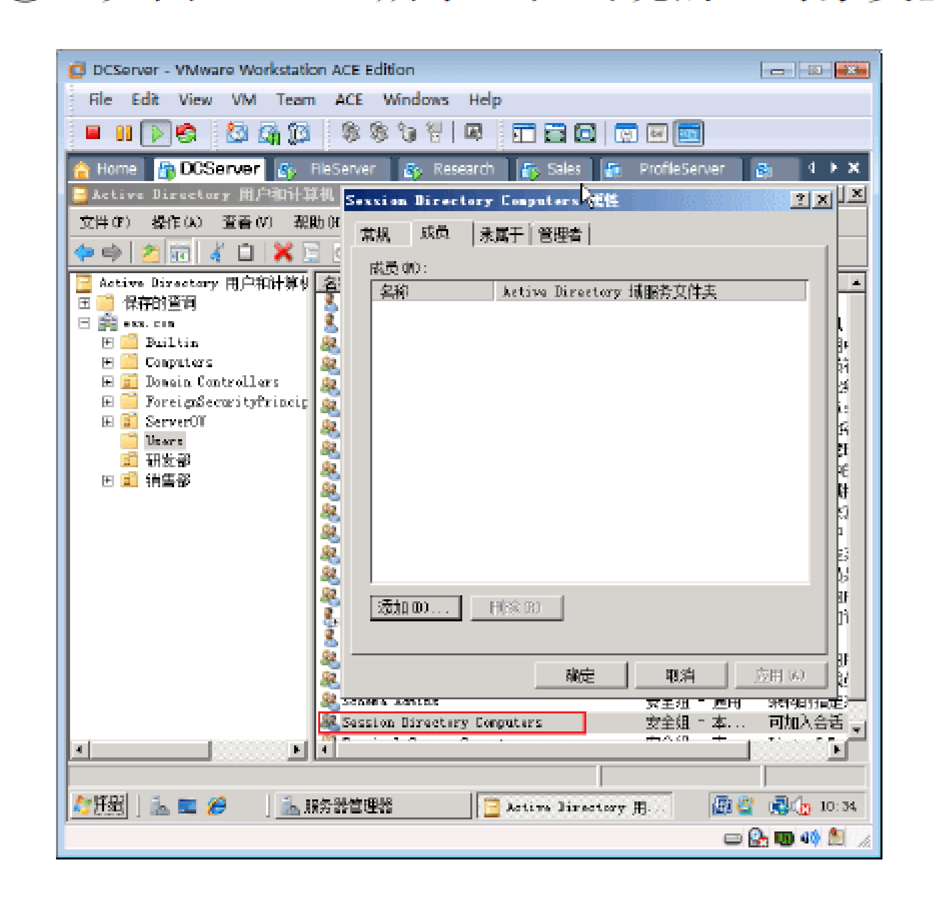


图 12-182　添加成员

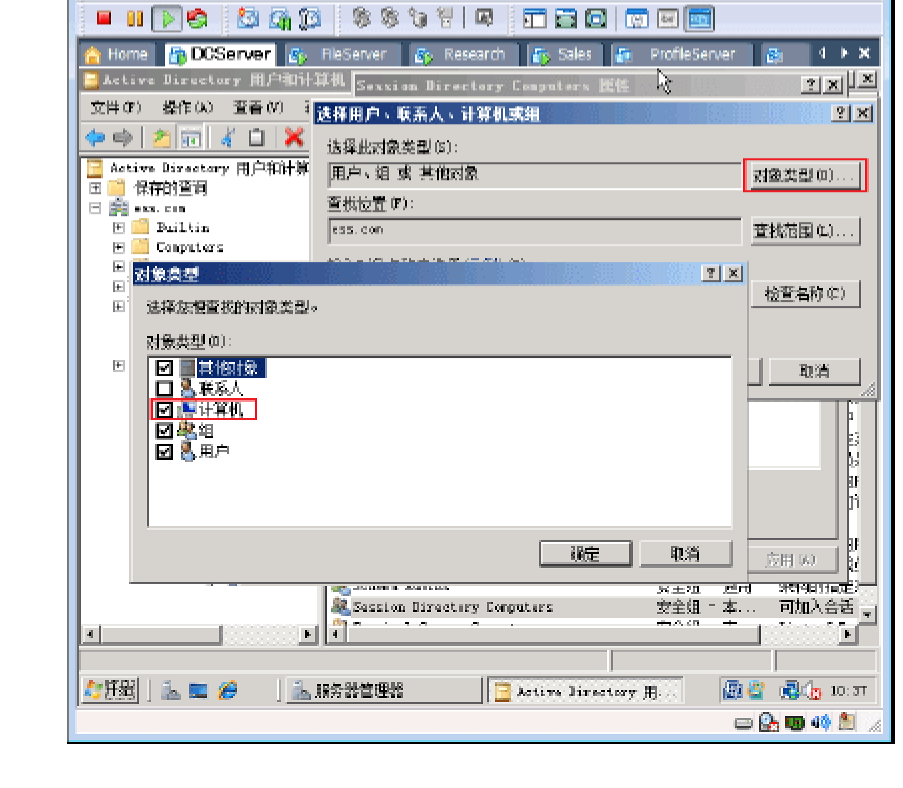


图 12-183　选择对象类型

⑦ 如图 12-184 所示，将 FileServer 和 Research 计算机账号添加到该组。

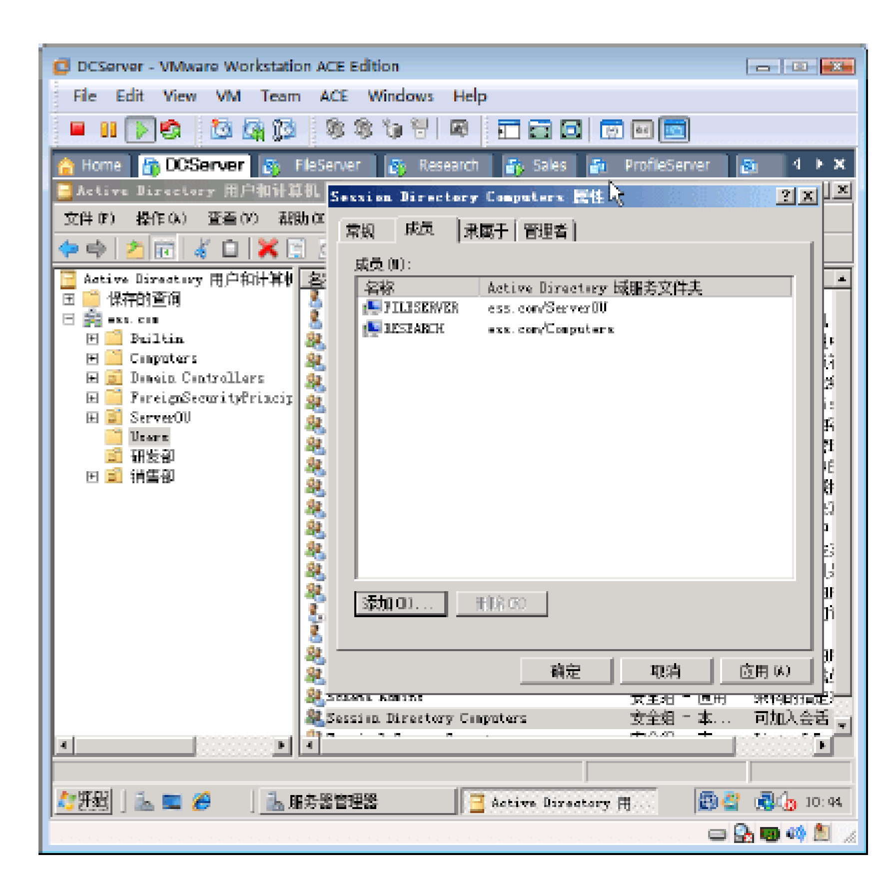


图 12-184　添加计算机到该组

12.9.2　任务 2：配置终端服务器使用 TS 会话 Broker

在 FileServer 和 Research 服务器上都安装终端服务，并配置使用 DCServer 作为 TS 会话 Broker。



注意：这两个服务器的终端服务端口必须一致。

① 在 FileServer 上，以域管理员账户登录。

② 选择“开始”→“管理工具”→“终端服务”命令，然后单击“终端服务配置”。

③ 如图 12-185 所示，双击“TS 会话 Broker 中的组成员”，在出现的对话框中，选中“加入 TS 会话 Broker 中的场”复选框，输入 TS 会话 Broker 服务器名或 IP 地址，输入 TS 会话 Broker 中的场的名称，选中“参与会话 Broker 负载平衡”复选框，选中“使用 IP 地址重定向”复选框，单击“确定”按钮，完成配置。

④ 如图 12-186 所示，同样在 Research 服务上指定 TS 会话 Broker。

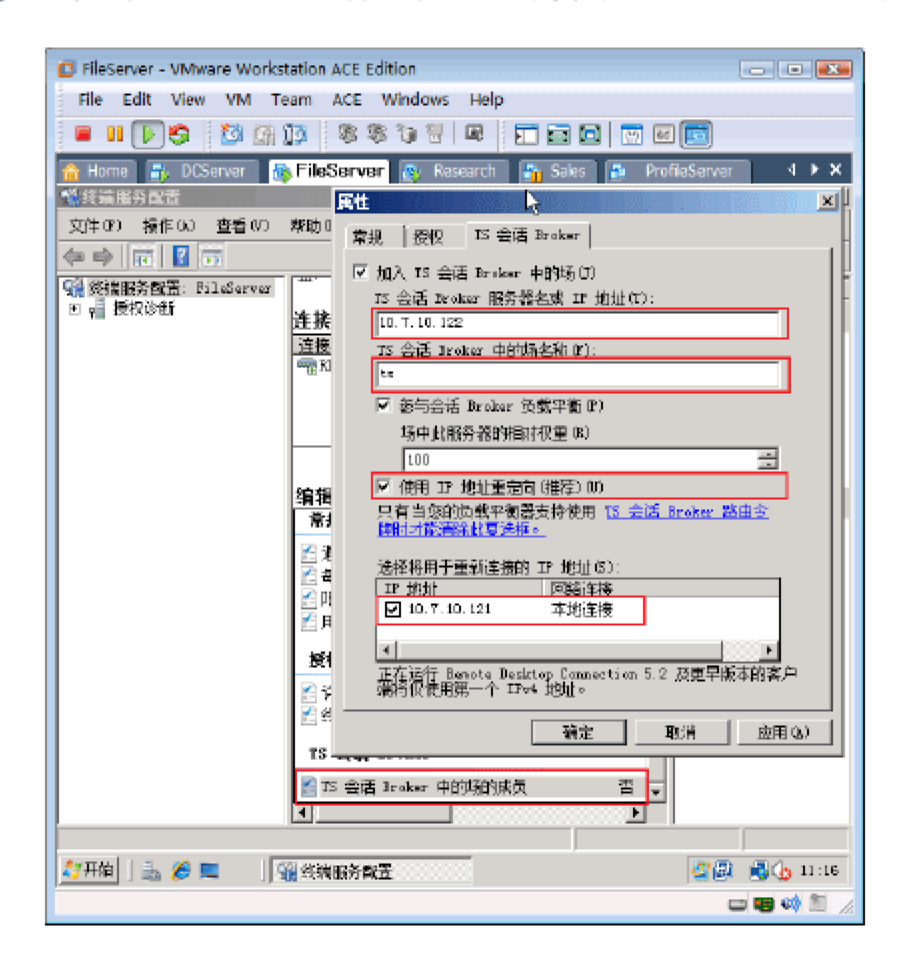


图 12-185　配置终端服务(一)

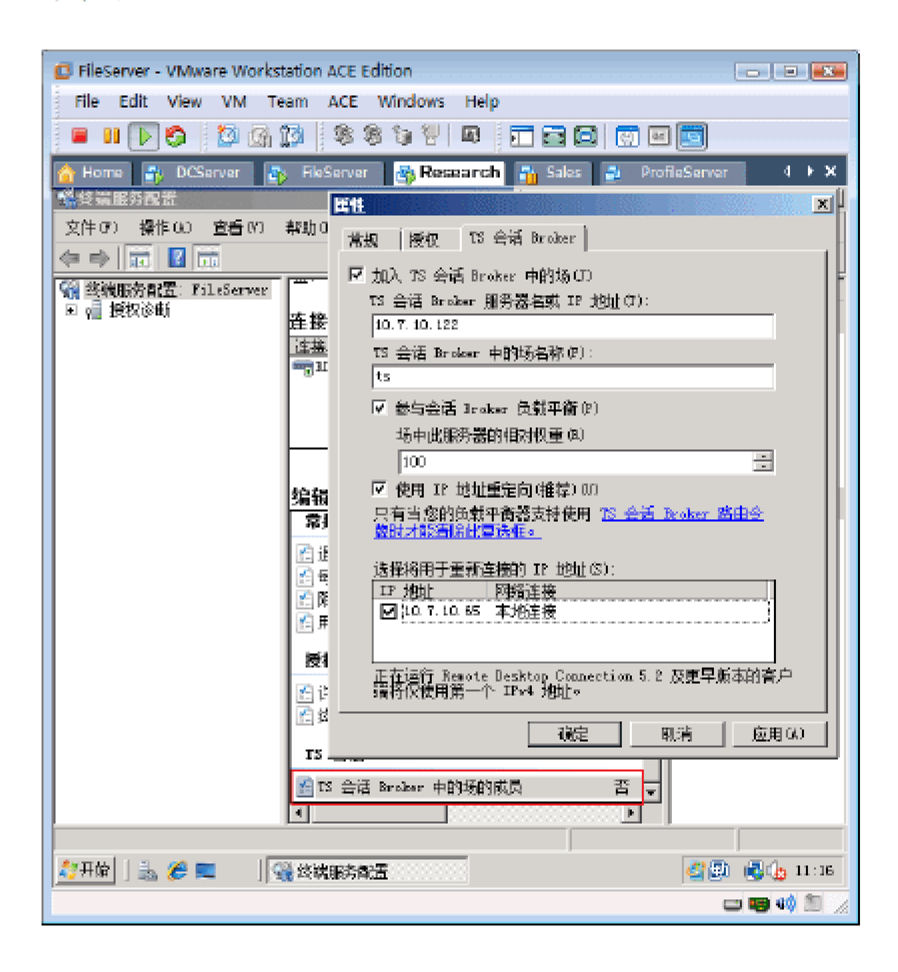


图 12-186　配置终端服务(二)

12.9.3　任务 3：为终端服务的名称解析配置 DNS

若要对终端服务器场中的会话进行负载平衡，可以结合使用 TS Session Broker 负载平衡功能和域名系统 (DNS) 循环。若要配置 DNS，必须为服务器场中的每台终端服务器创建一个 DNS 主机资源记录，将终端服务器的 IP 地址映射到 DNS 中的终端服务器场名称。

在基于 Windows Server 2008 的域控制器 DCServer 上配置 DNS

① 以域管理员的身份登录到 DCServer。

② 选择“开始”→“管理工具”→“DNS 管理器”命令。

③ 如图 12-187 所示，依次展开服务器名称、“正向查找区域”和域名。

④ 如图 12-187 所示，右击 ess.com，从弹出的快捷菜单中选择“新建主机(A 或 AAAA)”命令。

⑤ 如图 12-188 所示，在出现的“新建主机”对话框中，输入名称 ts 和 IP 地址 10.7.10.121，这是 FileServer 的 IP 地址。

⑥ 再次右击 ess.com，从弹出的快捷菜单中选择“新建主机(A 或 AAAA)”命令。

⑦ 如图 12-189 所示，在出现的“新建主机”对话框中，输入名称 ts 和 IP 地址 10.7.10.65，这是 Research 的 IP 地址。ts 就是场名。

场名称是客户端将用于连接到该终端服务器场的虚拟名称。不要使用现有服务器的名称。为了便于管理，建议使用与将终端服务器配置为加入 TS Session Broker 中的场时指定的场名称相同的场名称。

注意：默认情况下，在基于 Windows Server 2008 的域控制器上使用 DNS 时，将启用 DNS 循环。如图 12-190 所示，在 DNS 中查看服务器的属性时，可以在“高级”选项卡中配置“启用循环”设置。

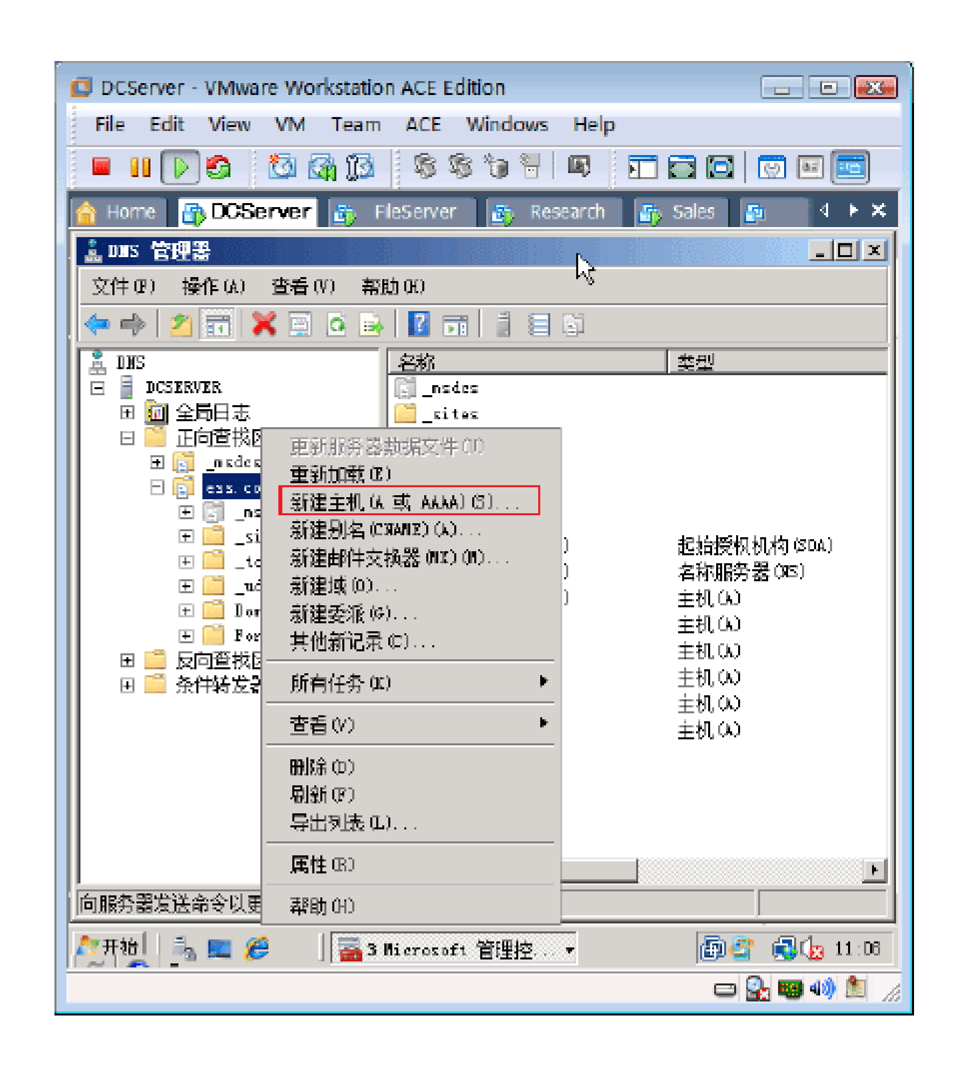


图 12-187　添加主机记录

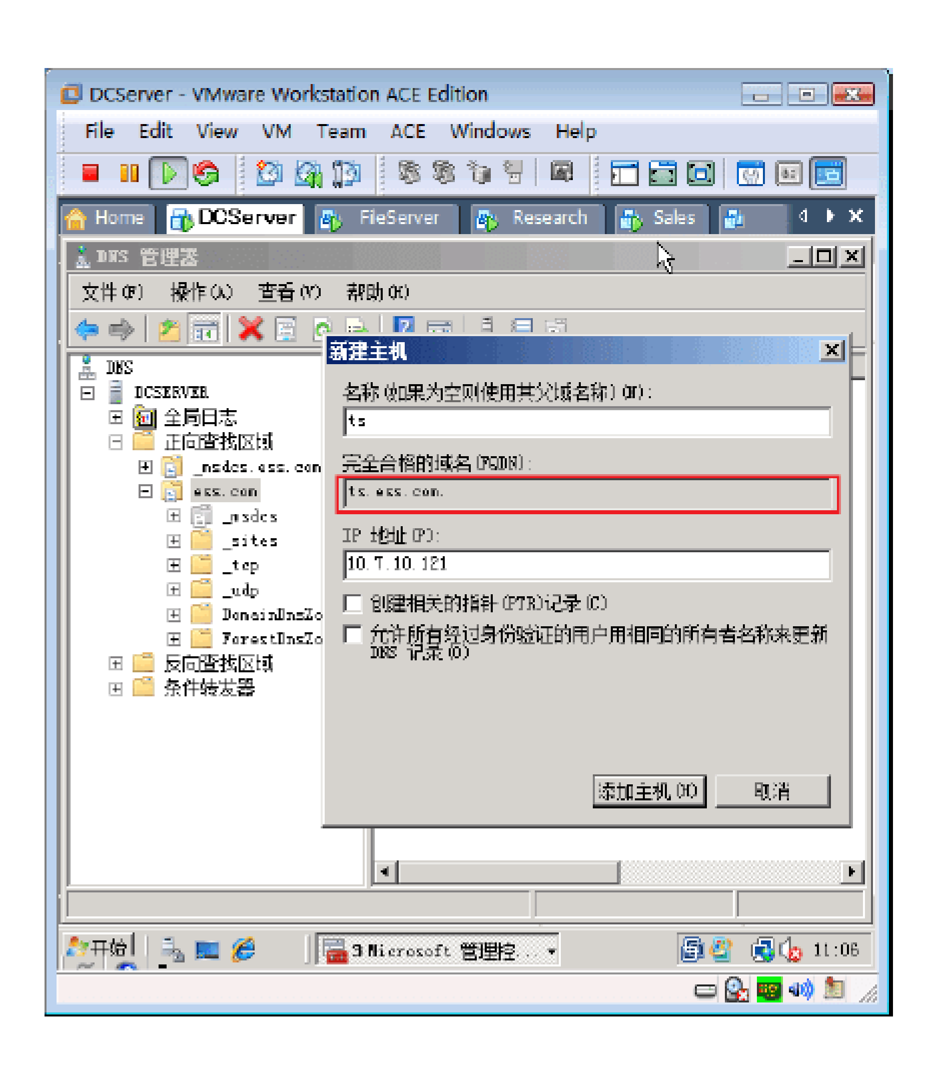


图 12-188　添加主机名称和 IP 地址

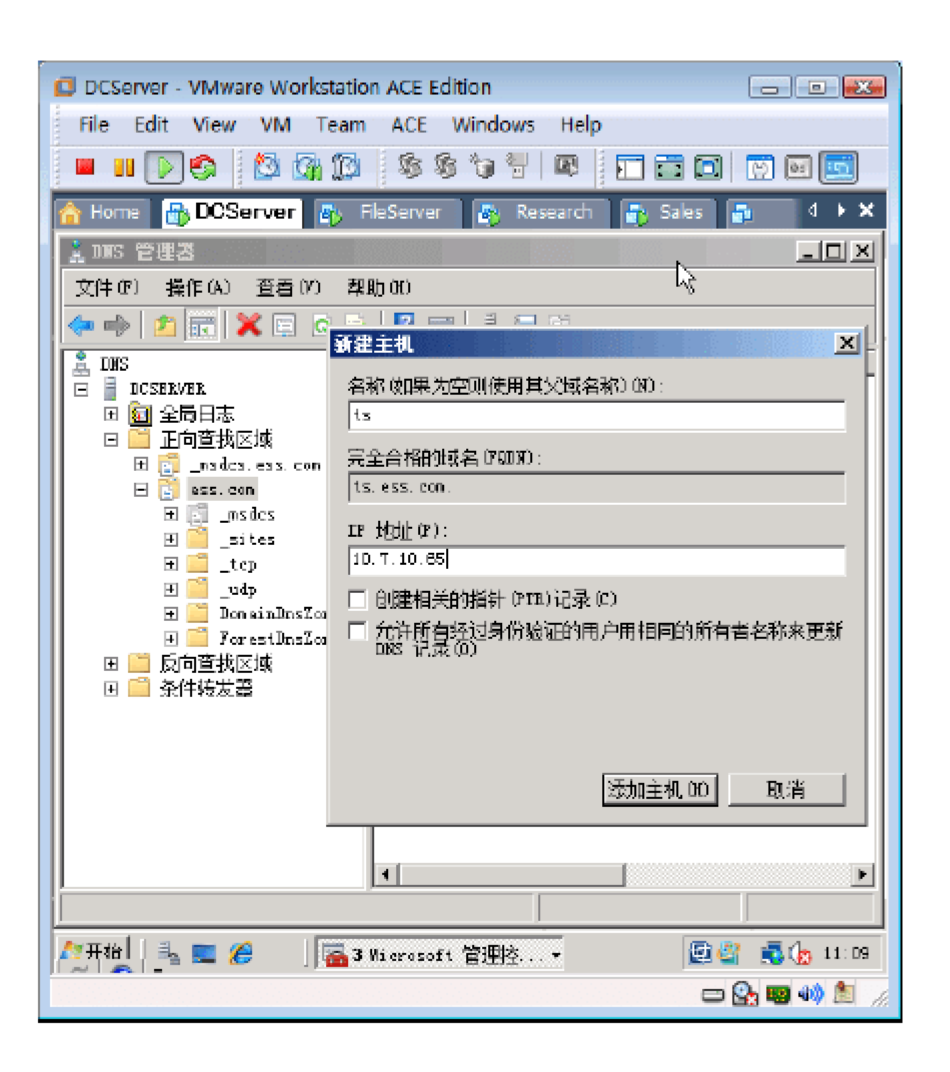


图 12-189　添加主机名称和 IP 地址

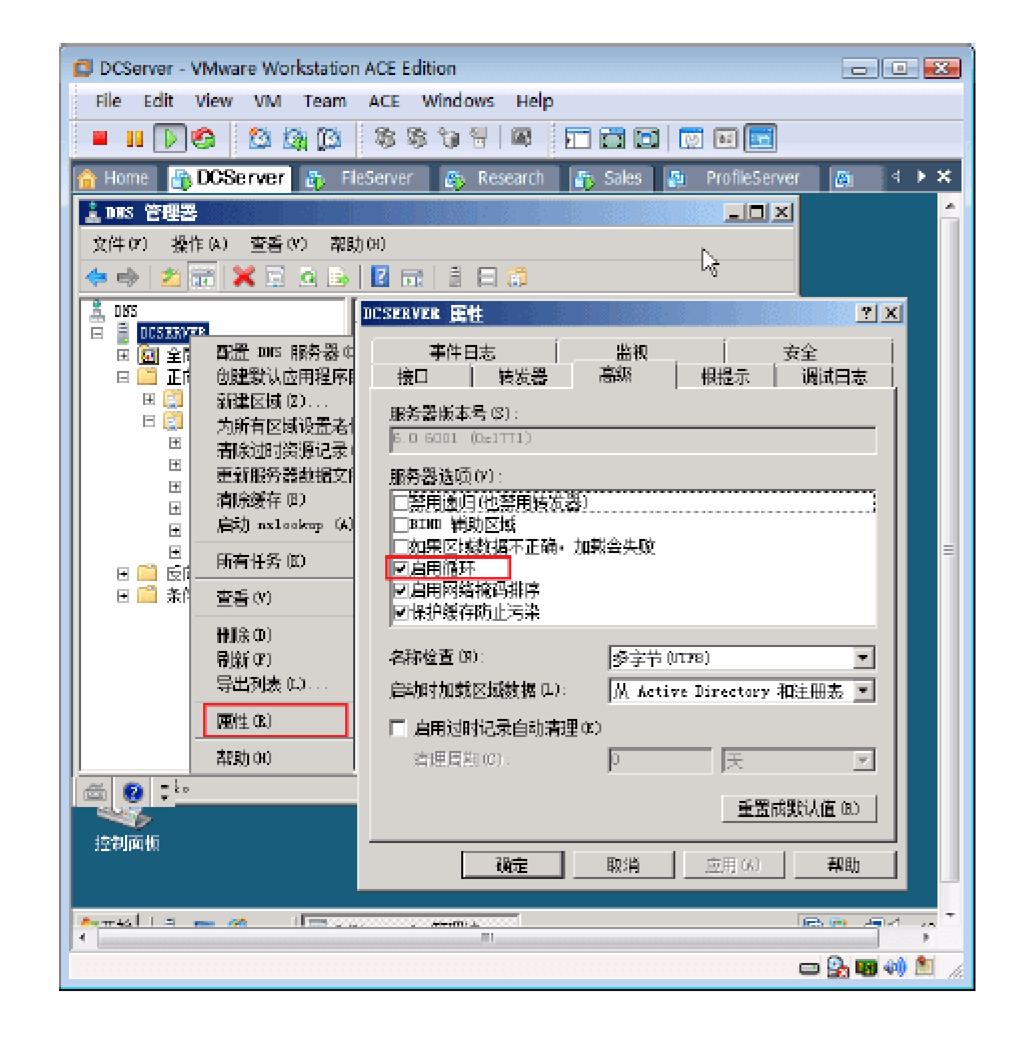


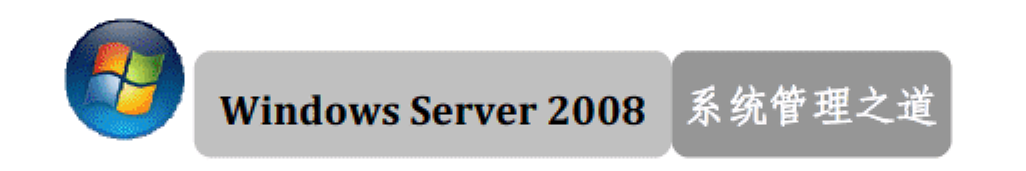
图 12-190　启用循环

12.9.4　任务 4：在 Sales 计算机使用连接终端服务

使用终端服务的场名连接到终端服务器场

① 如图 12-191 所示，以域用户的身份登录到 Sales 计算机。使用两个域用户连接 ts.ess.com 终端服务器场。

② 如图 12-192 所示，在命令行中输入 netstat -n，可以看到两个到终端服务器的会话，这两个会话



连接到了两个终端服务器。

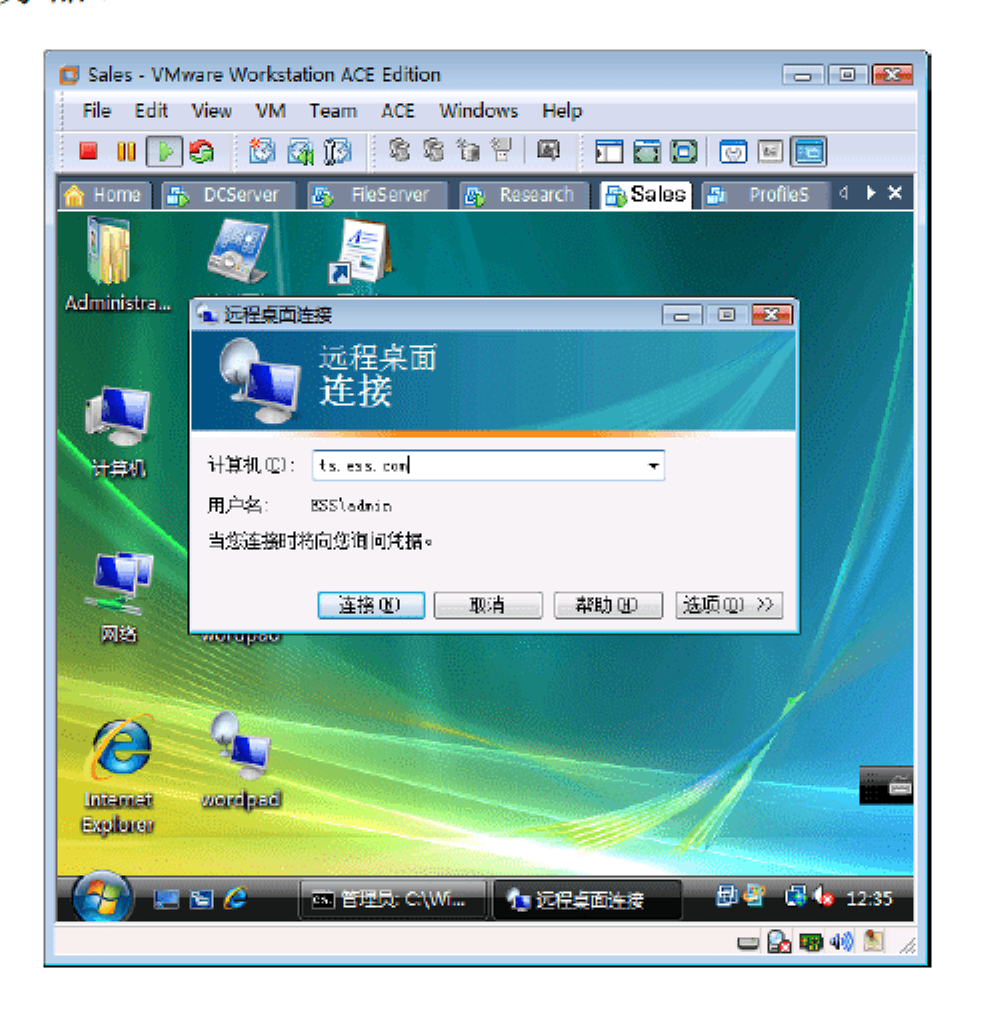


图 12-191　远程桌面连接(使用终端服务的场名)

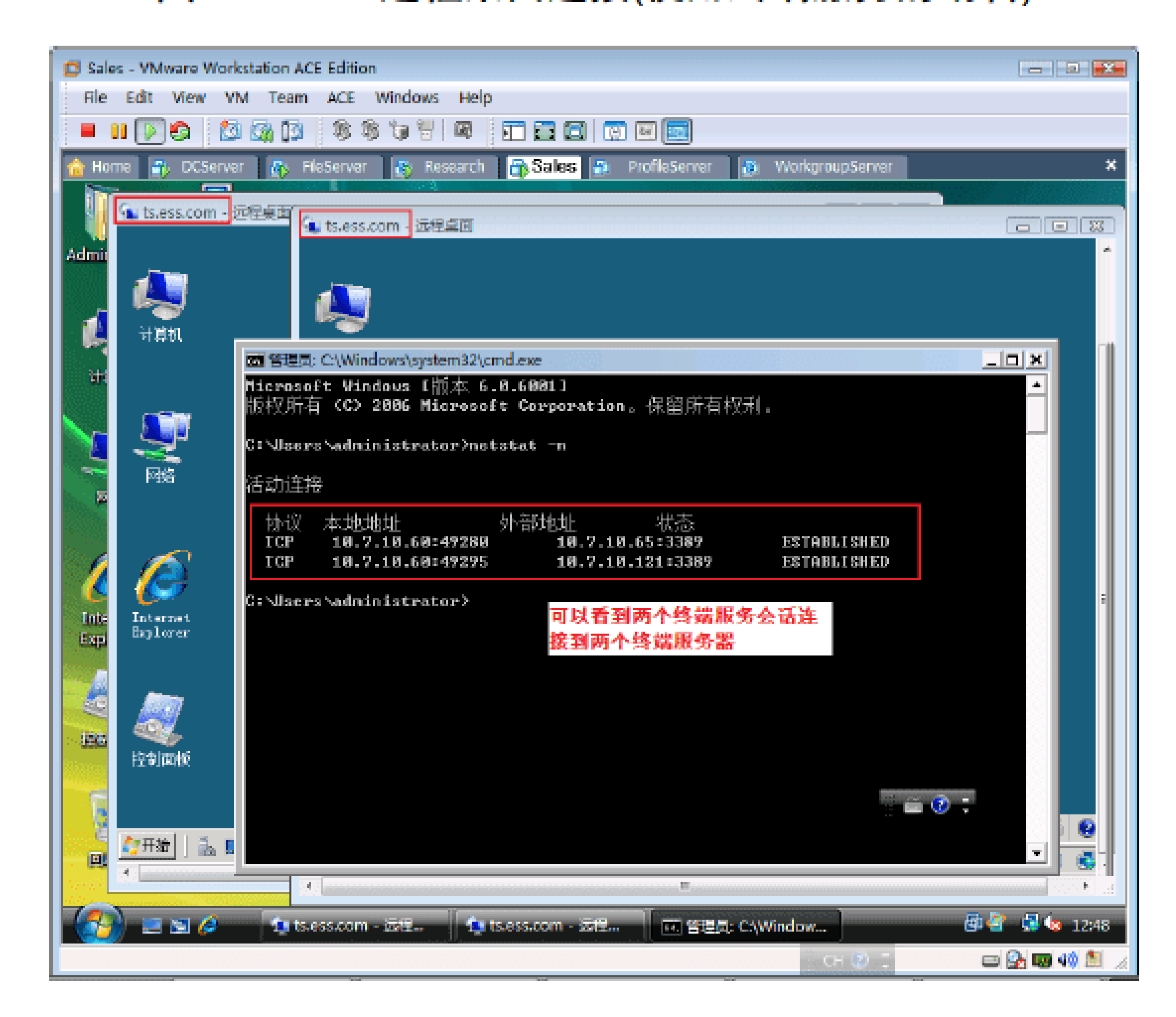


图 12-192　查看会话

第 13 章　Windows Server 虚拟化

如今，数据中心已经成为一个复杂的生态系统。在这个系统中，各种服务器、操作系统以及应用均可与各种桌面及移动客户端进行交互。IT 部门承受的压力越来越大，不仅需要管理与支持这类任务关键型技术，而且还要控制成本并保持高可靠性与安全性。采用服务器虚拟化技术——即可将不同的服务器移到集中管理环境中的虚拟机（VM）上——逐渐成了解决上述难题的理想选择。

关键词

- 虚拟化简介
- Windows Server 虚拟化结构
- 虚拟化技术对硬件的要求
- 安装 Hyper-V
- 创建和使用虚拟机
- 管理虚拟网络
- 虚拟化解决方案

13.1 虚拟化技术概述

虚拟化技术有助于显著降低 IT 成本、集中网络管理、增强网络安全性、改善服务器可用性，同时提高硬件利用率。虚拟化是企业服务器部署的必然趋势，如图 13-1 所示。

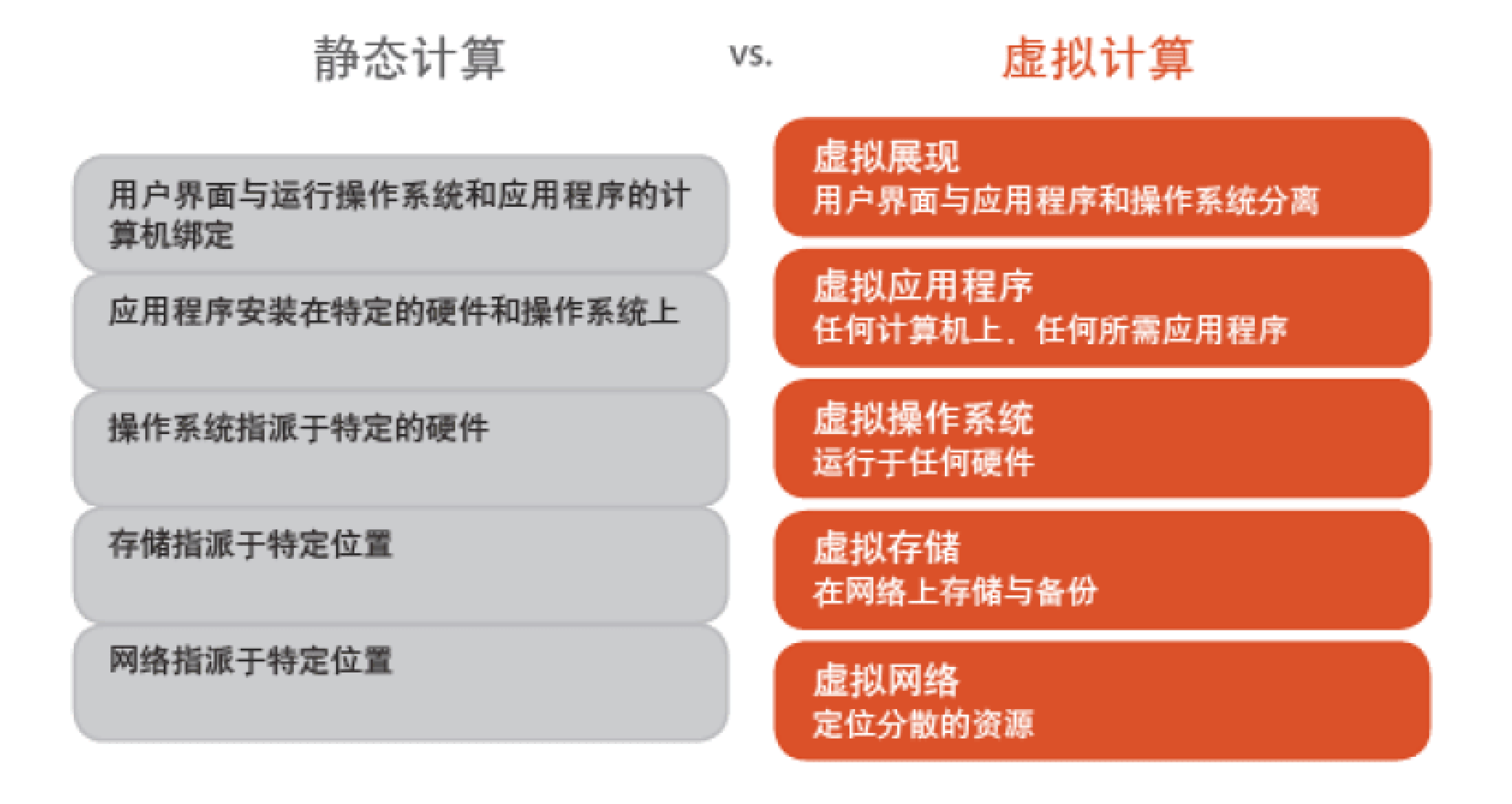


图 13-1 虚拟化技术

Windows Server 2008 包括 Windows Server virtualization (WSv)，这是一项功能强大的虚拟化与网络管理技术，使企业无须购买第三方软件即可充分利用虚拟化的优势。由于 VM 能够提供前所未有的功能来利用可用的硬件，微软及其合作伙伴可为解决各种操作系统(如：Windows、Linux 以及支持 Xen 的 Linux)之间的互操作性问题提供一站式支持，并且 IT 部门可以使用灵活性的、功能强大的工具来同时管理虚拟和物理资源。

本章介绍的 WSv 是微软桌面-数据中心虚拟化战略的重要组件。其中介绍了 WSv 中的新增与增强型功能如何帮助企业客户解决常见问题：服务器整合、业务连续性/灾难恢复管理、测试与开发以及动态数据中心。此外，本章还重点介绍了如何扩展这些优势来满足小型办公室与分支办公室的独特需求。

虚拟化是一项已经被广泛采用的解决方案。80% 的企业正在使用或评估虚拟化技术，并亲眼目睹了它在服务器整合、集中化管理及其他节约成本的应用中所表现出来的优势。由于这些优势可极大降低成本，因此企业希望将要求更为严格的工作负荷实现虚拟化。这些企业希望拥有功能更强大、更灵活的虚拟化解决方案，以更好地与其管理工具相集成。64 位多处理器多内核服务器的广泛采用激发了对能更好地利用高稳健性处理能力的 VM 需求。

为了适应这些发展，微软创建了 WSv，即新一代 64 位虚拟化技术，以促进对物理与虚拟组件进行灵活的无缝管理。该技术通过动态与可靠的虚拟化功能提供了支持平台的灵活性。

13.2 Windows Server virtualization 结构

1. 基于管理程序的虚拟化

Windows Server virtualization (WSv) 采用 64 位管理程序精心设计。该管理程序是常驻在操作系统与

硬件之间很薄的软件层。该管理程序可以在不发生冲突的情况下允许多个 VM 访问物理存储器与 CPU 资源。WSv 管理程序与虚拟化感知硬件(包括采用 Intel VT 与 AMD“Pacifica”技术的处理器)相结合，能够为来宾操作系统提供高性能与近乎无限的可扩展性。

2. 硬件虚拟化

由于 WSv 管理程序充分利用了 VT 与 Pacifica 技术，因此虚拟化多个操作系统的大部分工作均由系统硬件来执行，很少需要由虚拟化堆栈与管理程序来执行。

依赖于硬件的软件虚拟化平台必须频繁地中断来宾操作系统，中断的方式是将硬件请求随时转换成可与虚拟化环境兼容的形式。Intel VT 与 AMD“Pacifica”硬件技术可以通过将虚拟化扩展集成到 x86 结构中，消除许多不必要的随时转换工作。这意味着针对 VT 与“Pacifica”而设计的虚拟化平台具有更低的开销，并且 VM 运行效率也更高。硬件虚拟化特性与 WSv 的软件虚拟化组件之间进行协作，可以创建一款高性能的虚拟化平台。

3. 64 位结构

WSv 管理程序采用了 64 位设计。WSv 必须运行于 Windows Server 2008 x64 版之上，并能为 VM 提供近乎无限的可扩展性。与基于 32 位结构的虚拟化平台相比，WSv 的 64 位结构可提供更多的存储空间，WSv 主服务器可以容纳高达 1 TB 的物理 RAM。

用户可以为 WSv 托管的每个 VM 分配 64 GB 的 RAM。本章稍后将介绍 WSv 的动态硬件分配功能，该功能可以根据 VM 的资源需求将可变的 RAM 容量(多达 64 GB)分配给每个 VM 。这可以将要求更严格的工作负荷进行虚拟化，以便企业可以充分利用该功能来为多个来宾操作系统及 VM 提供宿主服务。借助资源分配方面的灵活性，可以将多个来宾操作系统整合到单个 WSv 主机上，每个操作系统在运行时几乎不会降低效率。

4. 64 位来宾操作系统支持

WSv 中使用的 64 位管理程序同时支持 32 位与 64 位来宾操作系统。有些应用程序可能仅存在于 32 位版本中，也有些应用程序可能仅存在于 64 位版本中(例如，LOB 应用可能在 32 位版本中，而 Microsoft Exchange Server 2007 仅可作为 64 位应用使用)。32 位与 64 位 VM 均可在同一 WSv 服务器上相互运行。同时容纳 32 位与 64 位 VM 的灵活性是 WSv 管理程序的主要优势。64 位 WSv 管理程序所创建的虚拟化基础可支持企业希望遵循的未来成长路线。

5. 操作系统分区

WSv 可以使用分区在多个 VM 之间分配主机系统硬件资源。分区是对包含单个操作系统的主服务器进行的逻辑分割。父分区包含虚拟化堆栈，用于管理子分区的内存与虚拟设备。子分区是指 VM。在 WSv 中，只能有一个父分区(Windows Server 2008 x64 实例或 Windows Server 2008 x64 的服务器内核安装)，但可以有无数个可配置的子分区。

父分区拥有连接到 WSv 主服务器的键盘、鼠标以及显示器。父分区还包含 Windows Management Instrumentation (WMI) 提供程序，能够简化虚拟化环境各方面的管理。此外，主机系统硬件所需的任何独立硬件厂商 (IHV) 驱动程序均包含在父分区中。子分区形成了操作系统、应用以及与 VM 相关的数据文件的逻辑容器。子分区具有对主服务器硬件有限的访问权限，并且必须通过称为 VMBus 的硬件共享模式来访问这一硬件，本章稍后将对此进行介绍。

6．微内核式（Microkernelized）管理程序架构

WSv 管理程序采用了与微内核操作系统相同的设计原理。特别是在对操作系统驱动程序及其他易受攻击的组件的执行权限级别较低这一方面，这意味着组件故障或受到攻击时对内核的损害有限或毫无损害。WSv 管理程序使用类似的设计方法来实现最小的可信计算基础（TCB），该基础没有任何自己的驱动程序(这些均包含在父分区与子分区中)。此微内核式管理程序结构可提供更稳定、更安全的基础平台来运行 VM，尤其是与基于单片管理程序的虚拟化平台相比较，该管理程序将硬件驱动程序集成到了管理程序代码库中。图 13-2 显示了 WSv 结构。

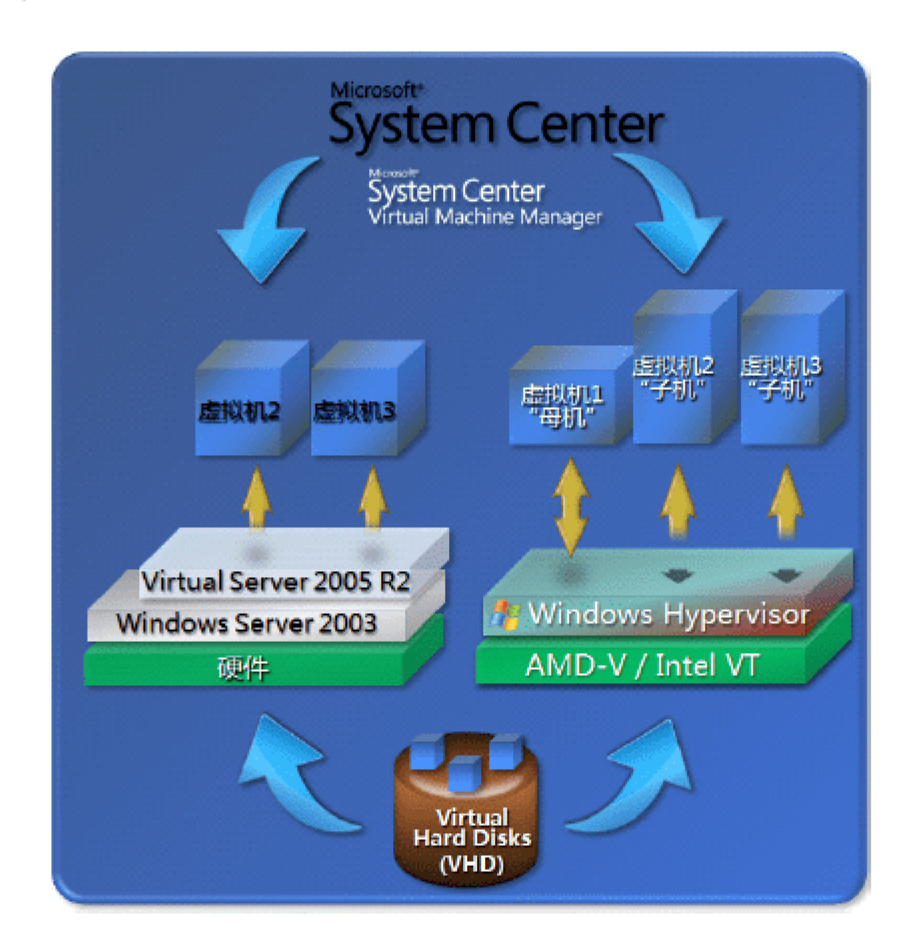


图 13-2　虚拟机技术架构

7．内存页面共享（Memory Page Sharing）

内存页面共享是一项 WSv 功能，可最大限度地提高 VM 内存使用的效率。当两个 VM 在内存中存储的页面完全相同时，WSv 将保留该页面的一个复制，并在来宾操作系统需要更改该页时才复制(copy-on-write）语义来简化对共享页面的更改。例如，在使用同一操作系统运行 10 个 VM 的 WSv 主机上，这些 VM 中很可能有许多共同的页面。WSv 可找到这些相同的页面并在所有 VM 之间共享通用页面。

页面共享的效率因工作负载同类或异类的程度不同而有很大差异。例如，10 个运行在同一操作系统的 VM 的页面共享效率比 10 个运行在 10 种不同操作系统的 VM 更高。页面共享可用于任何来宾操作系统，并可更高效地使用主服务器内存资源。

13.2.1　WSv 处理器支持

现代的服务器硬件可提供多种处理器配置选项。服务器主板上具有多个插槽（socket），可在其中插有多核处理器。WSv 处理器性能主要与可用处理器内核的数量及速度成比例。例如，插有双核处理器的两个插槽可以为 WSv 提供 4 个处理内核。

WSv 使用的处理器插槽数量由安装的 Windows Server 2008 版本确定。表 13-1 提供了支持处理器的一些示例。

表 13-1　按处理器配置与操作系统版本划分的支持处理器示例

处理器配置	父分区操作系统	效　果
两个插槽插有双核处理器	Windows Server 2008 Standard x64	父分区利用 4 个处理器内核 可为每个子分区分配多达 8 个逻辑处理器
8 个插槽插有双核处理器	Windows Server 2008 Standard x64	父分区利用 16 个处理器内核 可为每个子分区分配多达 8 个逻辑处理器
两个插槽插有双核处理器	Windows Server 2008 Enterprise x64	父分区利用 8 个处理器内核 可为每个子分区分配多达 8 个逻辑处理器
16 个插槽插有双核处理器	Windows Server 2008 Enterprise x64	父分区利用 8 个处理器内核 可为每个子分区分配多达 8 个逻辑处理器

备注：

Windows Server 2008 Standard Edition x64 能够利用多达 4 个处理器插槽。

Windows Server 2008 Enterprise Edition x64 能够利用多达 8 个处理器插槽。

Windows Server 2008 Datacenter Edition x64 能够利用多达 16 个处理器插槽。

WSv 能够为 VM 提供作为逻辑处理器的处理器内核。4 个插槽插有四核处理器的服务器包含 16 个处理内核，这 16 个处理内核可作为逻辑处理器提供给 VM。每个 VM 均可使用多达 8 个逻辑处理器进行配置。每个逻辑处理器可将该逻辑处理器上 VM 的计算负载转换成主服务器中物理处理器上的一系列的执行操作。

表 13-1 显示了几种可能的配置以及在每种配置中相应存在的处理器分配。子分区中安装的操作系统将决定可由该操作系统利用的逻辑处理器的数量。

13.2.2　全新的硬件共享结构

1. VMBus

WSv 采用了一种全新的硬件共享结构，该结构基于称为 VMBus 的跨分区通信通道。VMBus 是内存总线与分区间通信机制中的一种高速的点到点技术。主机与 VM 可使用 VMBus 这种机制来相互通信。如前所述，管理程序可以管理主机系统与 VM 以及主服务器的内存与处理器之间的交互。VMBus 管理磁盘、网络、输入/输出以及视频硬件交互。

2. Virtualization Service Providers (VSPs)

VSP 常驻在父分区中，并可与位于子分区中的 Virtualization Service Client (VMs) 主服务器硬件进行交互。VSP 可充当多路复用器，允许多个子分区共享硬件。例如，在具有 10 个 VM 但只有一个物理网络适配器的 WSv 主机上，父分区中的 VSP 能够确保所有这些 VM 均可成功并安全地共享同一个 NIC。WSv 具有用于存储、网络、输入与视频的 VSP。

3. Virtualization Service Clients (VSCs)

VSC 是来宾操作系统中的驱动程序，该操作系统可以通过在 VMBus 上与父分区中的 VSP 进行通信来间接地访问主服务器硬件。VSC 可提供完全假想的虚拟设备(并非仿真设备，后面将对此进行更为详细的介绍)，并通过 VMBus 与父分区中相应的 VSP(如：存储、网络、输入或视频)进行通信。有一组 VSP 在父分区中运行。每个子分区均运行自己的一套 VSC，VSC 能够与父分区中相应的 VSP 进行通信。

WSv 包括集成组件，这些组件取代了 Microsoft Virtual Server 2005 中使用的 VM Addition。Microsoft Virtual Server 2005 中的 VM Addition 用于增强来宾操作系统的性能(通过使用虚拟化感知软件组件来修补来宾操作系统)，并提供集成组件来支持各项功能，如从 Microsoft Virtual Server 管理界面中清除来宾关断功能。硬件辅助的虚拟化可取消不必要的来宾操作系统修补工作。集成组件可在 WSv 中执行这些任务，如图 13-3 所示。

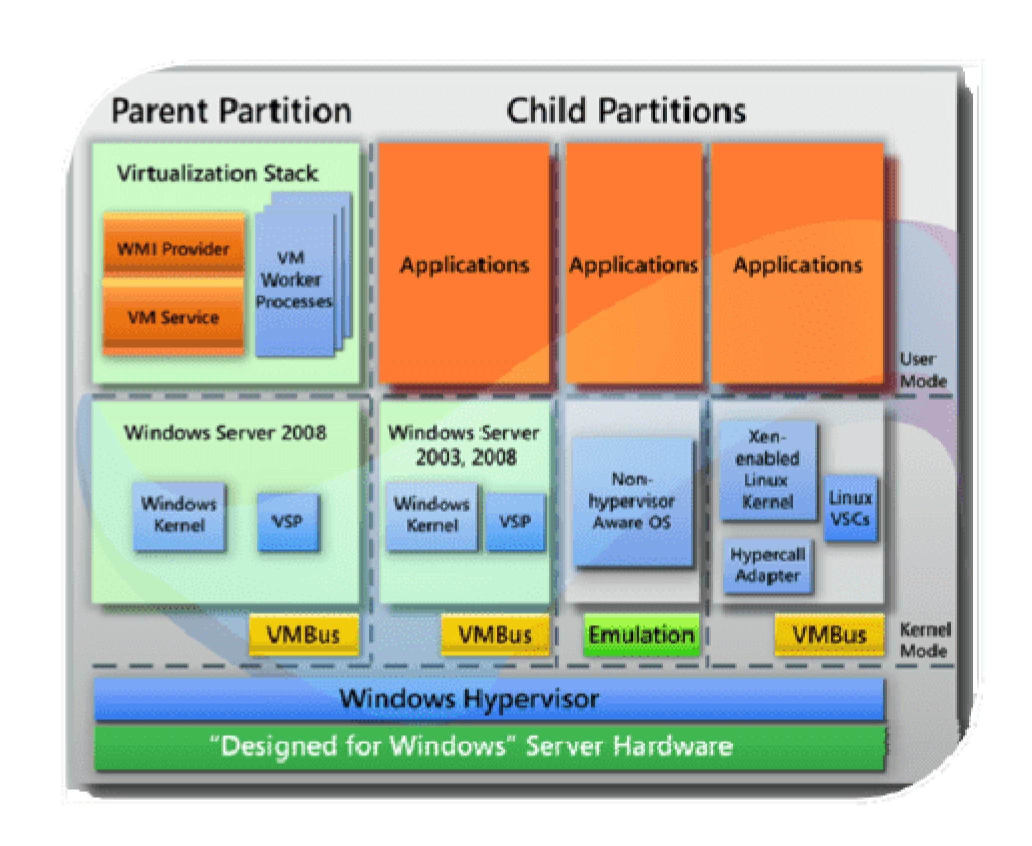


图 13-3　Hyper-V 架构

4. 假想设备(Synthetic Devices)

WSv 中的 VMBus 结构能够为来宾操作系统提供一种全新的硬件：假想设备。假想设备是映射到物理设备但并非仿真物理设备的虚拟设备。仿真的设备可以创建物理设备的真正软件代表。例如，对来宾操作系统来说，仿真的磁盘控制器与其物理副本无法分辨。这意味着来宾操作系统也同样会体会到其物理副本的限制。

假想设备可通过该操作系统集成组件包中的 VSC 提供给所有来宾操作系统。通常，基于 Windows 2000 Server 及更高版本的来宾操作系统可以使用假想设备。表 13-2 列出了为所支持来宾的操作系统提供的虚拟设备。

表 13-2　为所支持来宾的操作系统提供的虚拟设备

来宾操作系统	虚拟化设备类型
Windows 2000 Server SP4	网络适配器：假想 磁盘控制器：仿真
Windows Server 2003	网络适配器：假想 磁盘控制器：假想(仅在安装过程中为仿真)
Windows Server 2008	网络适配器：假想 磁盘控制器：假想(仅在安装过程中为仿真)
Windows XP	网络适配器：假想 磁盘控制器：仿真
Windows Vista	网络适配器：假想 磁盘控制器：假想(仅在安装过程中为仿真)
SUSE Enterprise Linux	网络适配器：假想 磁盘控制器：假想

13.2.3 存储功能

WSv 推出了几项与 VM 存储硬件相关的新功能。在 Microsoft Virtual Server 中，VM 的文件内容存储在一个或多个虚拟硬盘（VHD）文件中。主机操作系统在可访问的文件系统、典型的内部硬盘存储器或存储域网络（SAN）上维护这些 VHD 文件。WSv 支持以全新的方式访问来宾操作系统的存储器。

1. VM 的传递磁盘访问

传递磁盘访问（Pass-Through Disk Access）允许 VM 在不使用 VHD 文件的情况下直接访问可编写的文件系统。例如，具有 SQL Server 数据库、运行 Windows Server 2008 的 VM 可以使用传递磁盘访问来访问位于 iSCSI 或光纤通道 SAN 上的数据库文件。此外，还可对此 VM 进行配置，以访问直接连接到 WSv 主服务器的磁盘上的分区。

使用传递磁盘访问使得非虚拟化系统也能访问通常以 VHD 格式封装以便在文件系统上进行处理的数据。存储配置中的这一额外选项为 WSv 使用场景增添了灵活性。例如，虚拟化 SQL Server 可能会使用传递磁盘访问在 SAN 上存储其数据库文件，这样，报告应用也可访问这些文件。在另一个示例中，虚拟化 IIS 7.0 Web 服务器可能会使用传递磁盘访问在 SAN 上存储 Web 内容，这样，内容索引应用也可以访问这些文件。

2. 全新的存储设备控制器结构

WSv 中使用的 VMBus 结构能够为 VM 提供假想存储设备控制器。假想存储设备控制器支持高达 255 VHD/控制器，并且每个 VM 支持无数个控制器。基于 Windows Server 2003 或更高版本以及 Windows XP 或更高版本的来宾操作系统可以利用假想存储设备控制器。

不支持假想设备的来宾操作系统将使用仿真 IDE 控制器来进行存储访问。Microsoft Virtual Server 2005 中的仿真 SCSI 控制器已删除。这是因为仿真 IDE 控制器已修改，克服了以前的局限性。WSv 中的全新仿真 IDE 控制器具有与 Microsoft Virtual Server 2005 中的仿真 SCSI 控制器相同类型的功能。

13.2.4 强大稳健的网络

1. VLAN 支持

WSv 充分使用虚拟开关来控制进入与退出 VM 的网络通信量并确保其安全。WSv 虚拟开关可与物理网络虚拟 LAN (VLAN) 标记关联，以限制通过该虚拟开关与指定 VLAN 的网络通信。可以将多个 WSv 虚拟开关与单个物理网络适配器关联。WSv 中的 VLAN 支持可以通过限制从 VM 到指定 VLAN 的网络通信为 VM 提供更高的网络安全性。

2. PXE 引导

WSv 中的虚拟网卡支持预引导执行环境（PXE）启动。这一网络启动使得客户能够以类似物理服务器的方式来配置其 VM。为了利用这一功能，需要在主机网络上使用 PXE 基础设施。

3. VM NAP 支持

WSv 可与 Windows Server 2008 中的网络访问保护（NAP）功能配合使用，能够防止有害的 VM 访问企业网络并危及其安全。NAP 可用于配置与实施计算机正常运行状态要求，并在不符合要求的计算机连接

到公司网络之前进行更新或修正。借助 NAP，管理人员可以配置正常运行策略，以定义软件要求、安全更新要求以及连接至企业网络所需的配置设置等。

NAP 可通过评估客户机的正常运行状态并在计算机不符合要求时限制网络访问来实施正常运行要求。客户端与服务器端组件均可协助修正不符合要求的计算机，以使它们能够获得不受限制的网络访问。如果计算机确定为不符合要求，则可以拒绝它访问该网络，也可以立即对其进行修正，使其符合要求。

NAP 实施方法支持四种网络访问技术，这些技术可与 NAP 配合使用来实施正常运行策略：Internet 协议安全性 (IPSec) 实施、802.1X 实施、支持路由与远程访问的虚拟专用网 (VPN) 实施以及动态主机配置协议 (DHCP) 实施。

NAP 的优势在于其应用于 VM 的方式与应用于环境中的物理计算机的方式相同(第 5 章中对 NAP 进行了更全面的介绍)。

13.2.5 基于角色的灵活安全性

在运行多个 VM 的 WSv 上使用基于角色的安全性意味着限制一个或多个 VM 管理员的访问权限。例如，管理角色可能是企业市场部的数据库管理员。通过以非虚拟化配置方式运行的专用数据库服务器，可以为数据库管理员分配访问数据库服务器，而非企业内任何其他服务器的权限。

由于非虚拟化服务器通常利用率不高，因此企业将把以前部署在专用服务器上的工作负载整合到整合型服务器上。在上面的示例中，可能将营销数据库服务器整合至运行其他数据库与应用程序的服务器上。这种整合难以确保服务器的安全性，因为多个管理员仅拥有访问所需 VM 需要的访问级别，而不具备对主机服务器或其他 VM 的管理访问权限。在此示例中，营销数据库管理人员只能访问和管理营销数据库 VM。

利用 WSv，可以为工作负载(如营销数据库)分配其自己的 VM 。由于虚拟机的安全界限与分立物理服务器相同，因此可以为营销数据库管理人员分配对存放市场数据库的虚拟服务器的管理访问权限，而不赋予他们对主机或组织机构内其他虚拟服务器的管理访问权限。

WSv 中的这项功能使整合服务器更为轻松与灵活。

13.2.6 服务器核心上的 WSv

WSv 可作为角色安装在服务器核心上。服务器核心为运行一个或多个以下服务器角色提供了环境。

- WSv。
- 动态主机配置协议 (DHCP) 服务器。
- 域名系统 (DNS) 服务器。
- 文件服务器。
- Active Directory® 目录服务 (AD DS)。
- Active Directory 轻量级目录服务 (AD LDS)。
- Windows Media Services。
- 打印管理。

在服务器核心上运行 WSv 可提供下列额外的安全性与性能优势。

- 减少攻击面：由于服务器核心使用了一组最少的 DLL 与系统组件，因此可以减少遭到攻击与安全威胁的可能性。在 Windows Server 2008 的服务器核心安装中不存在通常成为攻击目标的应

用，如 Internet Explorer。

- 降低软件更新要求：服务器核心提供了一组更少的服务器角色。由于服务器上未提供的角色不必通过软件更新来进行维护，因此服务器核心需要的 Windows 更新下载更少，频率也更低。服务器核心的额外优势在于频率更低的重新引导，因为 Windows 更新需要强制重新引导。
- 性能：服务器核心的内存尺寸非常小，同时也是运行 WSv 的平台中开销最低的。

由于 WSv 的 MMC 3.0 管理控制台能够轻松地从工作站或另一个 Windows Server 2008 服务器创建并管理 VM，因此服务器核心可能是众多 WSv 安装的 Windows Server 2008 理想配置。WSv 中的 WMI 提供程序(在本章后面部分进行讨论)与 PowerShell 脚本支持能够为主机服务器与来宾 VM 基于脚本的管理提供强大而灵活的支持。

13.2.7 灵活的资源控制

WSv 能够以可控制的灵活方式在运行的 VM 之间分配资源。Microsoft 虚拟服务器能够为 VM 分配固定的 RAM 容量。WSv 扩展了这一功能，包括动态 RAM 分配。借助于动态 RAM 分配，可以为 VM 分配最低保证的 RAM 量以及所需的 RAM 量。

1. 内存分配

WSv 包括的新功能可用于管理分配给虚拟机 VM 的内存。在 WSv 中，使用内存分配来配置 VM。连同此配置设置一起，还可配置内存保留设置。内存保留是保证为 VM 提供的内存分配的一部分。例如，如果将 VM 配置为 8 GB 的内存，并具有 75% 的内存保留，则在 VM 启动时将为其分配并保证提供 6GB 的物理 RAM。剩余的 2 GB RAM 可能作为物理 RAM 页面(如果存在)分配，否则将对其进行磁盘可调页配置。

WSv 的内存保留功能特别适用于性能不太重要的测试与开发环境。在来宾操作系统性能非常重要的情况下，建议将内存保留设置为 100%。

WSv 内存保留功能提供的灵活性使得管理员能够在测试与开发环境中获得更高的虚拟机密度。

2. CPU 资源分配

WSv 能够使用灵活的 CPU 资源分配模式在运行的虚拟机之间分配主机服务器物理 CPU 资源。表 13-3 介绍了 WSv CPU 资源分配计算中使用的设置。

表 13-3 CPU 资源分配设置

项 目	说 明
相对权重	VM 相对于所有其他 VM 的资源需求赋予的相对权重。根据需要可以从相对权重较低的其他 VM 为相对权重较高的 VM 动态分配额外的资源。默认情况下，所有 VM 的相对权重均为 100，因此它们的资源要求相同，没有任何优先顺序。管理员可以为每个 VM 分配的相对权重为 1～10 000。在大多数情况下，这是唯一需要进行配置的设置
保留的容量(一个 CPU 的百分比)	为此 VM 保留的单个 CPU 的容量。为 VM 提供的 CPU 容量百分比绝不能小于此值
最大容量(一个 CPU 的百分比)	在任何给定时间此 VM 可占用的单个 CPU 总资源的最高百分比
保留容量(系统百分比)	为此 VM 保留的总体系统 CPU 容量的百分比

续表

项　目	说　明
最大容量(系统百分比)	在任何给定时间此 VM 可占用的总体系统 CPU 资源的最高百分比
保留的总容量	为所有当前正在运行的 VM 保留的物理计算机的总 CPU 容量。如果物理计算机具有多个 CPU，则此数字表示所有 CPU 保留的百分比之和
剩余的可用容量	未为所有当前正在运行的 VM 保留的物理计算机的总 CPU 容量。如果物理计算机具有多个 CPU，则此数字表示所有可用 CPU 的百分比之和

备注：WSv 提供了其自己的资源管理器，以便为 VM 分配系统资源。其他资源管理器(如：Windows System Resource Manager)不应与 WSv 一起使用。

13.2.8　WSv 的高可用性

WSv 包括可与故障转移群集配合使用的增强特性，以确保在 Windows 虚拟运行的 VM 上具有高可用性。在与故障转移群集及 System Center Virtual Machine Manager 一起使用时，WSv 使得管理员能够以最少的服务中断响应计划停机的需求及对意外停机做出回应。

WSv 使用以下功能实现高度可用的 VM。

- 故障转移群集。
- Quick Migration。
- 备份。
- 群集与 WSv。

Windows Server 2008 群集通过在出现意外或计划停机时允许 VM 迁移到群集中的其他节点，来实现 WSv 的高可用性。群集实现的方式有：对 WSv 角色本身进行群集(如主机群集)，或者对以 WSv 方式运行的各个 VM 进行群集(如来宾群集)。

1. 主机群集

使用 Windows Server 2008 故障转移群集可实现 WSv 角色高度可用性，这意味着一个或多个运行 WSv 的服务器添加了故障转移群集角色，并以受支持的群集配置进行了配置。这就是主机群集。故障转移群集的主要要求是对群集节点共享存储。可能包括 iSCSI 或光纤通道存储域网络 (SAN)。所有 VM 均存储在共享存储区域中，并且由一个 WSv 节点来管理正在运行的 VM 状态。在发生计划停机时，可以使用 Live Migration 功能(本章稍后介绍)将运行的 VM 移到另一个群集节点上。在发生意外停机时，群集服务将在现存的群集节点上自动重新启动 VM。主机群集能够为整个 WSv 平台以及常驻在 WSv 服务器上的所有 VM 提供高可用性。

2. 来宾群集

可使运行于 WSv 中的 VM 群集化，即使基本主机操作系统并非两个，或可配置的更多 VM 的情况下也如此，这样，VM 中的来宾操作系统就能够访问存储群集资源的外部共享存储器。如果来宾操作系统支持群集，则它们经过配置后可以为群集资源提供高可用性。

使用 WSv 来宾群集可以为数据库、文件共享、网络基础架构与应用服务等大量资源提供高可用性。WSv 来宾群集可以与 Windows Server 2008 网络负载均衡 (NLB) 服务相结合，以便多个 WSv 主机服务器同时提供高可用性与负载均衡。

NLB 是一种功能，其可在 NLB 群集中跨多个服务器为网络客户端与服务器应用分配负载。NLB 对确保无状态应用(如在 Internet 信息服务 (IIS) 上运行的基于 Web 的应用)在工作负载增加时通过添加额外的服务器对其扩展尤为有用。在负载增加时，NLB 允许添加额外的服务器来实现可扩展性。此外，NLB 还允许用户轻松替换故障服务器来实现可靠性。

3. WSv 与 Geo-clustering

在 Windows Server 2008 故障转移群集中，取消了小于 500 ms 的网络时延要求。现在，时延要求为可配置的。在 Windows Server 2008 中，群集可以跨越子网。这就不需要像以前一样要求使用 VLAN 来连接地理位置分散的群集节点。

Windows Server 2008 中 Geo-clustering 的改进使得用户能够将数据中心操作故障转移到与主站点相隔一段距离的恢复站点。

4. WSv Quick Migration

利用 WSv Quick Migration 功能可以将正在运行的 VM 从一个 WSv 主机移到另一个主机。主机群集配置支持 Quick Migration，能够提供 Quick Migration 所需的基本共享存储管理与资源再分配技术。

管理 Quick Migration 的方式有三种。其中之一是，System Center Virtual Machine Manager (SCVMM) 提供一个 GUI 界面，允许正在运行的 VM 从一个 WSv 主服务器拖放迁移到同一群集中的另一个主服务器。如果未使用 SCVMM，则可以使用故障转移群集管理器 (MMC) 控制台来初始化正在运行的 VM 从一个 WSv 主服务器 Quick Migration 到同一群集中另一个主服务器的过程，同时最大限度地缩短停机时间。WSv 中的 WMI 提供程序还可以对上述过程的 Quick Migration 编写脚本。Quick Migration 的速度取决于内存中必须移动的信息量以及共享存储设备的速度。

13.2.9　管理功能

1. Virtual Server Migration

Microsoft Virtual Server 2005 与 WSv 利用通用的开放式 VHD 格式来存储虚拟机的文件内容。这意味着在 Virtual Server 2005 中创建的现有 VM 可以迁移到 WSv 主机上。管理员可以在 Virtual Server 2005 中创建与管理现有的虚拟化工作负载，并在部署之后，将这些 VM 直接移到 WSv，而不必重新创建 VM。这可以确保管理员能够继续利用其在虚拟化基础设施方面的现有投资，并在准备就绪后将该基础设施移到 WSv 上。

2. WMI 提供程序

WSv 可通过 Windows Management Instrumentation (WMI) 进行管理。WSv WMI 提供程序可控制 WSv 所有方面的对象，其中包括：

- 管理服务器设置。
- 创建与配置 VM。
- 创建与配置虚拟网络开关。
- 控制正在运行的 VM 状态。

此外，WMI 提供程序还允许外部脚本编写与管理工具(如 Windows PowerShell、System Center Virtual Machine Manager 及其他第三方工具)管理 WSv 服务器。

3. 组策略集成

管理员可以使用组策略来管理在 Windows Server 2008 与 Windows Server 2008 服务器核心上运行的 WSv 服务器的全局设置。这样就可以使用管理员所熟悉的现有管理工具对 WSv 服务器组进行集中管理。

4. 性能计数器

WSv 提供了一组详细的性能与资源利用率计数器，这些计数器能够按全局或按每个 VM 报告资源的使用情况。这些性能计数器使得管理员能够确定 VM 使用主服务器资源的方式。这一信息可以帮助管理员隔离 WSv 环境中的性能问题，并最高效地将 WSv 主机服务器硬件分配给 VM。WSv 虚拟化计数器还能提供源数据进行退款清算。

5. 关键故障通知

WSv 采用关键故障通知来识别危急情况并做出相应回应。例如，WSv 主机服务器可能配备了不间断电源 (UPS)。在出现停电时，UPS 将向父分区发出信号告知电源已断，并告诉父分区预期电池使用寿命还有多长。WSv 能够以各种方式来响应这一关键故障通知。WSv 可以做出以下响应之一。

- 保存状态并关闭 VM 电源。
- 关闭来宾操作系统。
- 不保存状态即关闭 VM 电源。
- 如果对 WSv 主机进行了相应配置，则启动 Live Migration。
- 来宾操作系统支持。

业务部依赖于动态数据中心为每项业务职能提供最高效的工具，即使这些工具要求独特的硬件或软件配置。例如，依赖于制造工艺且基于 Linux 的垂直应用应能与其他领域基于 Windows 的应用共存。

WSv 支持运行 Windows、Linux 与支持 Xen 的 Linux 的 64 位及 32 位 VM，以及支持与大多数主要操作系统兼容的 32 位 VM。以前专用于单一应用功能的服务器可以替换为采用动态硬件管理与故障转移群集等先进功能的 VM。

6. 正在进行的 VM 热备份

WSv 可与 Windows Server 2008 中的 VSS 进行交互，以允许备份正在运行的 VM。这意味着在服务器开始将其 VHD 文件复制到备用位置时，可以对正在运行的整个服务器进行备份。

7. WSv 联机备份

WSv 具有集成的 VSS 编写器组件。VSS 编写器组件包含在可提供一致卷影副本的应用程序与服务中。当应用程序与服务正在运行时，编写器可与卷影复制服务(通常由备份程序调用)配合使用，以确保在创建卷影副本时不对卷执行写入操作。此技术允许在 VM 联机并运行时创建备份。

8. WSv 灾难恢复准备工作

借助 WSv，在灾难恢复准备时可以使用比非虚拟化服务器及某些其他产品更多的选项。由于管理员可以备份正在运行的 VM，因此无须关闭虚拟服务器即可对其进行系统备份。这便为管理员的备份计划提供了更大的灵活性。

如果 WSv 主服务器出现故障，则该主机上的所有 VM 将无法使用，直到主服务器修复或替换。如果管理员已将该主机的 VM 备份到备用位置，则备份的 VHD 文件包含将 VM 恢复到备份点所需的全部信

息。如果有一个 WSv 服务器具有未使用的硬件容量，则可以将该备份虚拟机还原到此备用服务器，然后接通 VM 电源，恢复服务。尽管此灾难恢复方法应经过测试，以确定辅助服务是否会受此还原操作类型影响，但它提供了一种从影响 WSv 主机的灾难中快速恢复的出色可选方法。

9. VM 快照

WSv 可与 Microsoft Volume Shadow Copy 服务相集成，以使管理员能够创建正在运行的 VM 的时间点（point-in-time）快照。这在备份与灾难恢复的情况下非常有用。此外，当管理员需要实施复杂或高风险的配置更改时也极为有用，因为一旦情况不妙，他们还可以选择回滚这些更改。在管理员创建 VM 的快照时，WSv 可在拍摄快照之前确保 VM 处于一致的状态。

13.3 创建虚拟机

本节将会演示在 64 位的 Windows Server 2008 上安装虚拟机，管理虚拟机，设置虚拟机网络，创建虚拟机快照等操作。

13.3.1 安装 Hyper-V

在 64 位的操作系统上，安装 Windows Server 企业版，在 BIOS 中启用对虚拟化技术的支持。安装 Hyper-V 角色，打上最新的 Hyper-V 补丁。



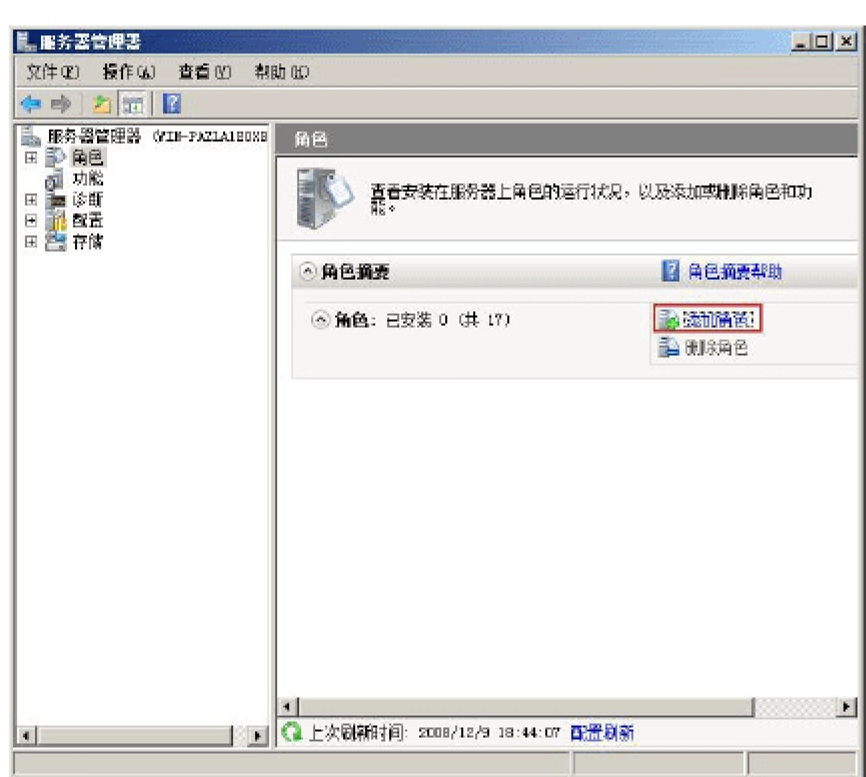
提示：以下操作在 Dell D630 系列笔记本电脑上进行。

① 设置笔记本 BIOS，启用 CPU 对虚拟技术的支持。

② 启动计算机。

③ 打开服务器管理器，如图 13-4 所示，单击“添加角色”按钮。

④ 如图 13-5 所示，在弹出的“开始之前”界面中，单击“下一步”按钮。



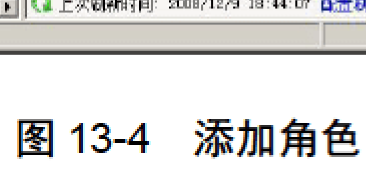


图 13-4 添加角色

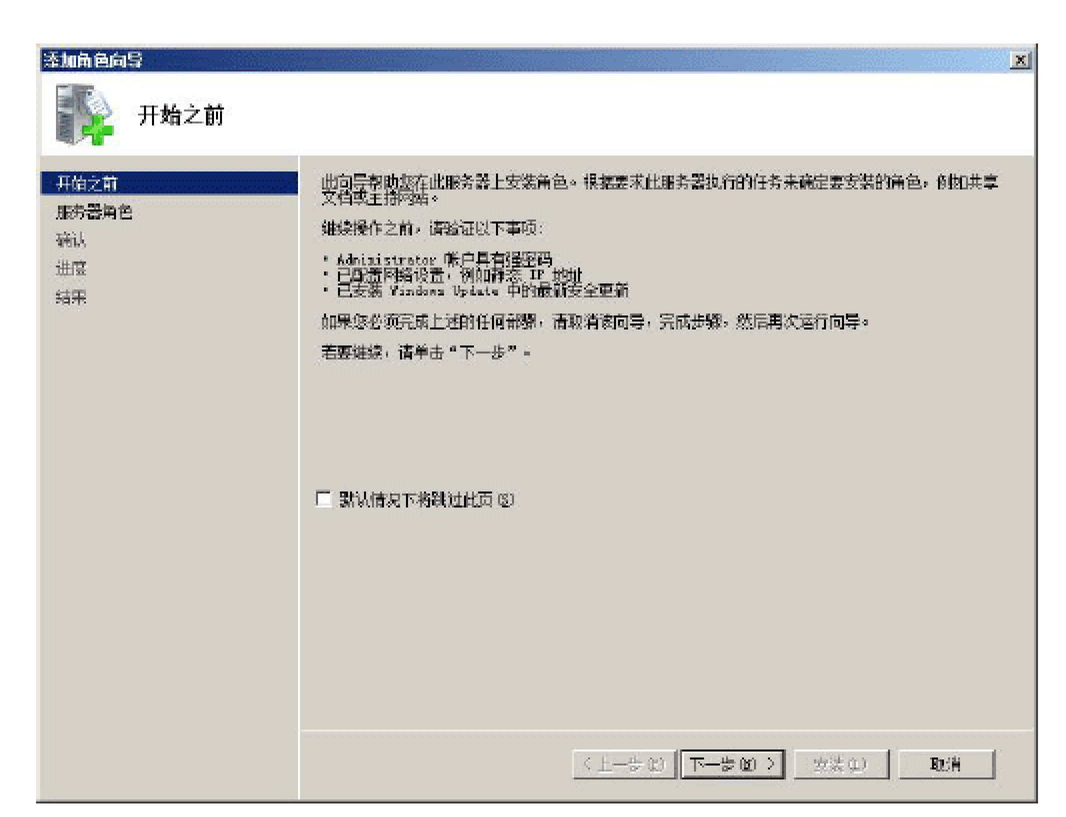


图 13-5 添加角色向导

⑤ 如图 13-6 所示，在出现的“选择服务器角色”界面中，选中 Hyper-V 复选框，单击“下一步”

按钮。

⑥ 如图 13-7 所示，在出现的 Hyper-V 界面中，单击“下一步”按钮。



图 13-6 选择角色

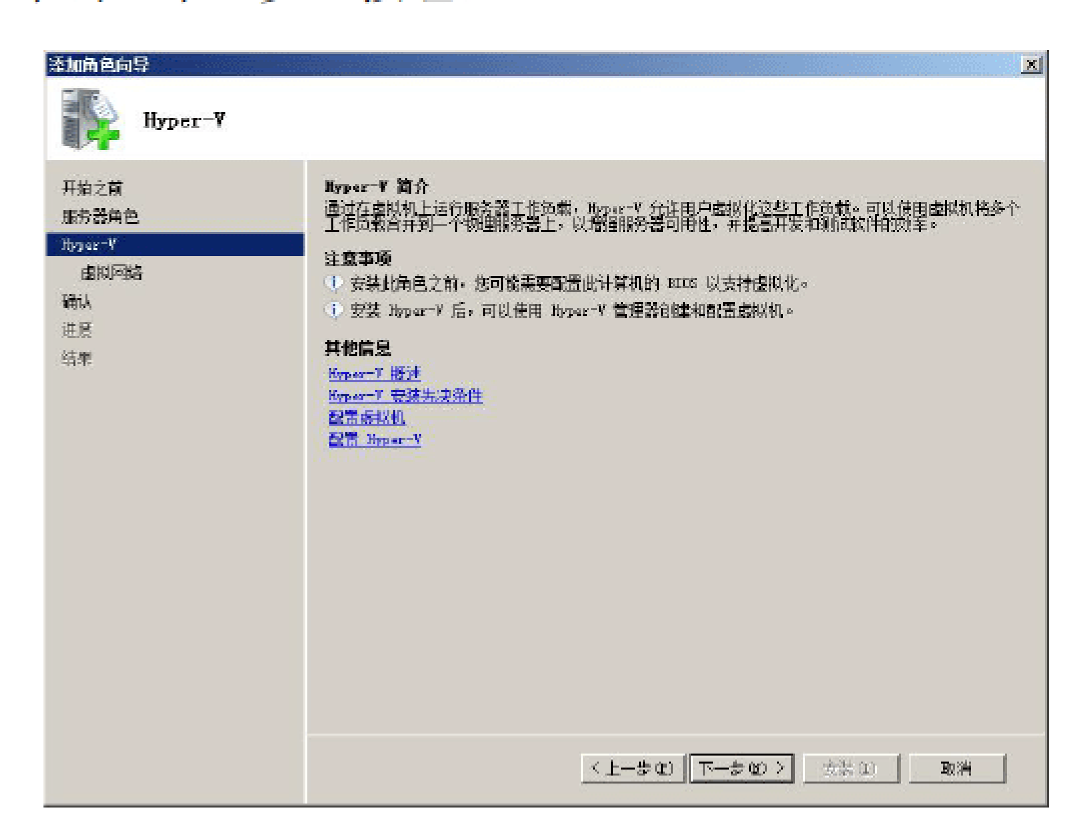


图 13-7 Hyper-V 介绍

⑦ 如图 13-8 所示，在出现的“创建虚拟网络”界面中，选中“本地连接”复选框，单击“下一步”按钮。

⑧ 如图 13-9 所示，在出现的“确认安装选择”界面中，单击“安装”按钮，完成 Hyper-V 角色的安装。

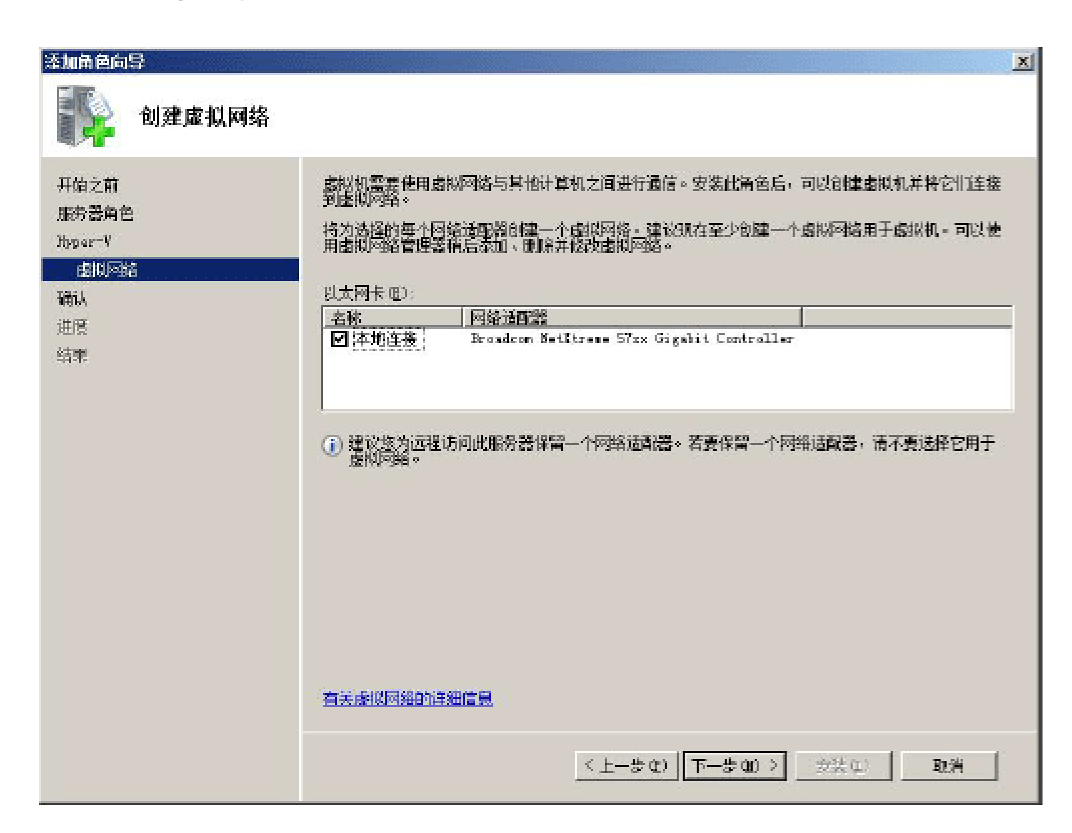


图 13-8 创建虚拟网络

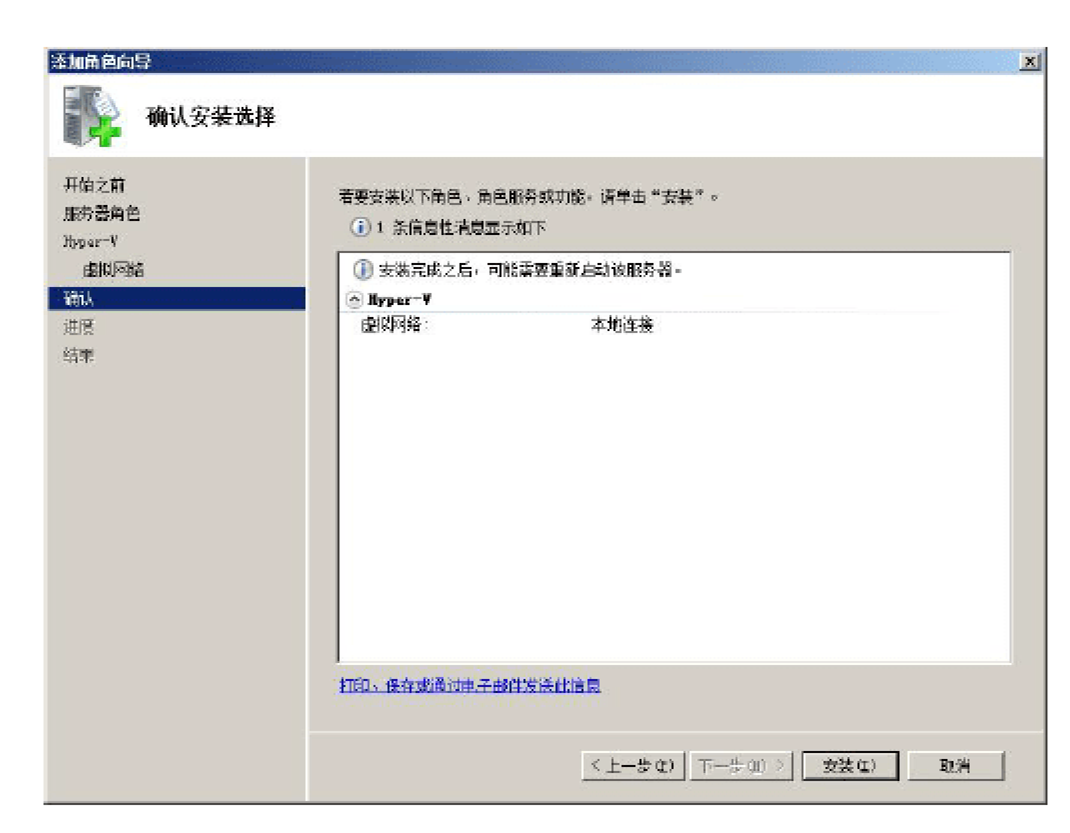


图 13-9 确认安装

⑨ 从微软站点下载下列 Hyper-V 补丁，依次双击安装。

Windows6.0-KB952627-x64.msu
Windows6.0-KB951636-x64.msu
Windows6.0-KB950050-x64.msu

13.3.2 Hyper-V 设置

在安装虚拟操作系统前，先更改 Hyper-V 的常规设置，更改虚拟机默认位置。

① 打开 Hyper 管理工具，如图 13-10 所示，右击服务器，在弹出的快捷菜单中选择“Hyper-V 设置”命令。

② 如图 13-11 所示，单击“虚拟硬盘”，可以更改虚拟硬盘的位置到一个较大的磁盘分区，单击“确定”按钮。

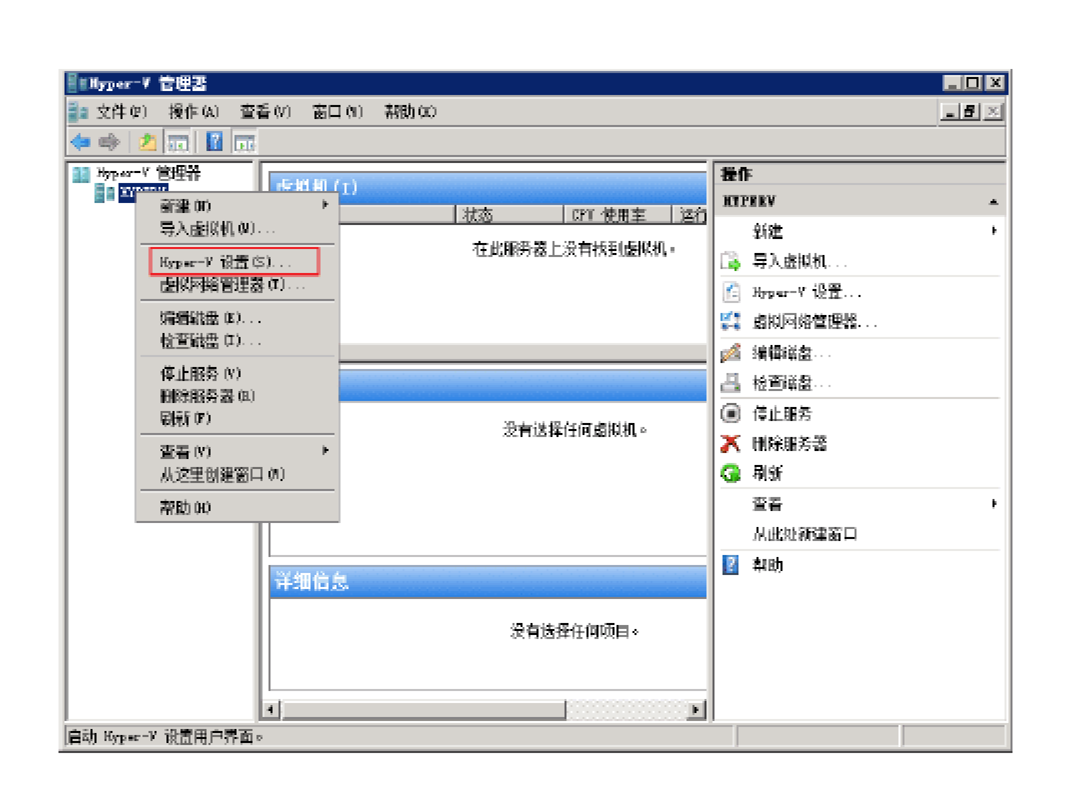


图 13-10　配置 Hyper-V

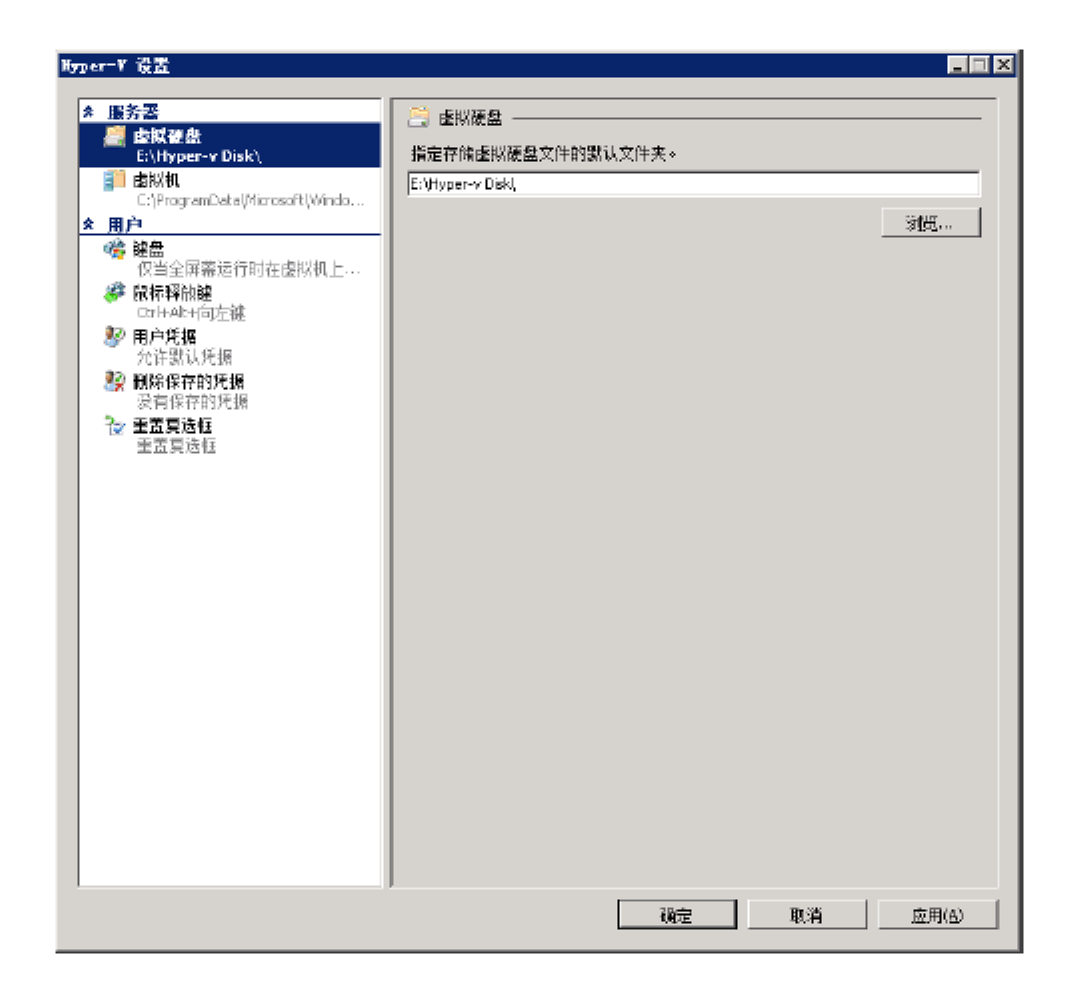


图 13-11　更改虚拟硬盘

③ 如图 13-12 所示，单击“虚拟机”，可以更改虚拟机配置文件的默认文件夹路径，单击“确定”按钮。

④ 如图 13-13 所示，单击“键盘”，指定当运行虚拟机连接时，指定 Windows 键组合发送给虚拟机还是物理机。

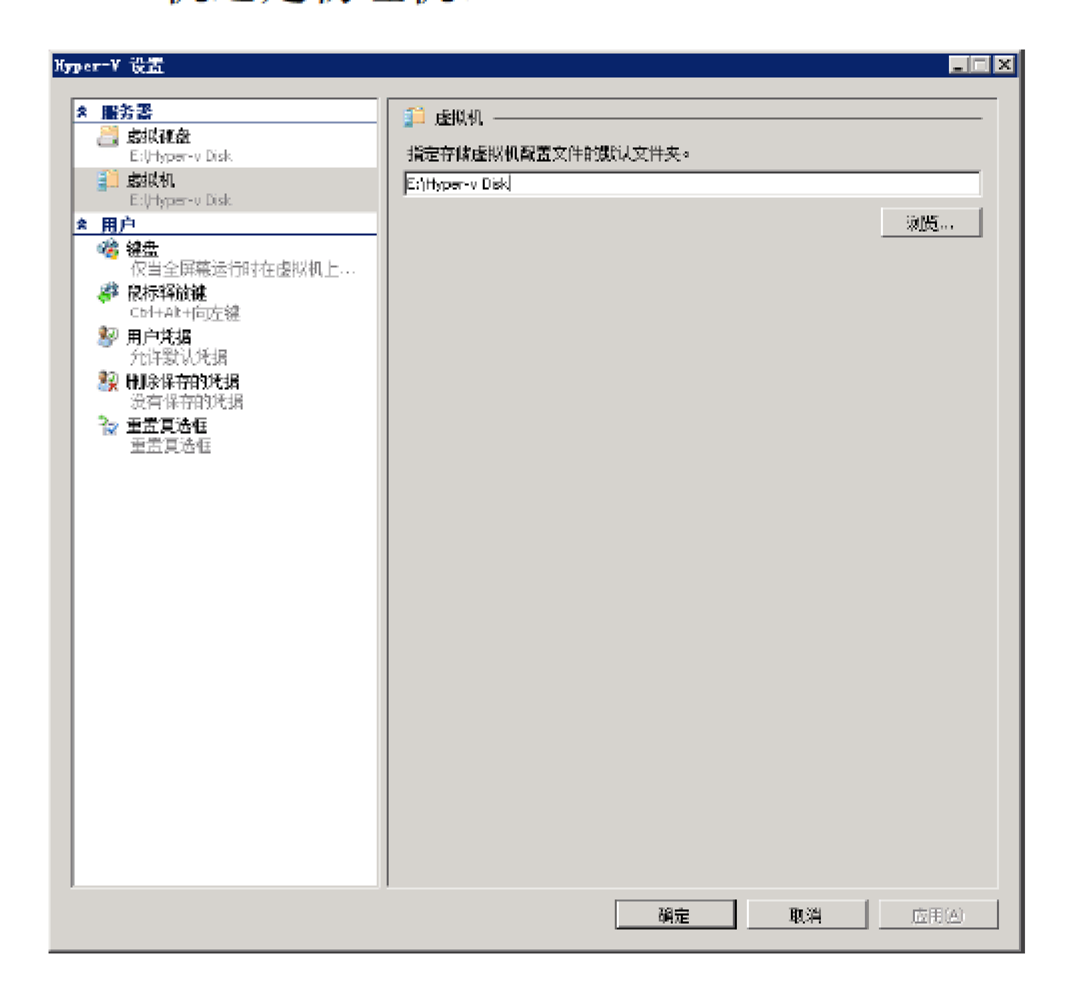


图 13-12　虚拟机配置文件的默认位置

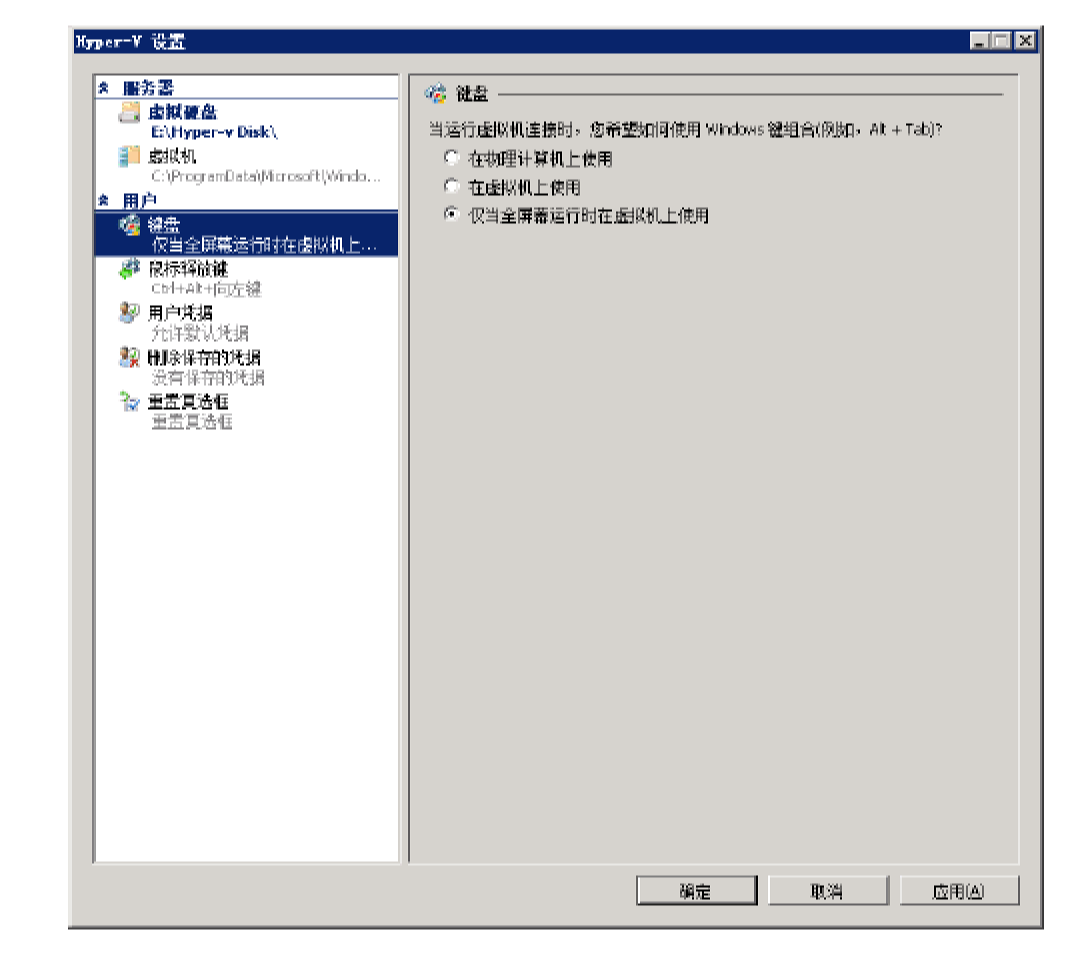


图 13-13　设置键盘

⑤ 如图 13-14 所示，单击“鼠标释放键”，指定当未安装虚拟机驱动程序时希望用于释放鼠标的键组合。

⑥ 如图 13-15 所示，单击“用户凭据”，指定是否希望对虚拟机连接自动使用默认凭据连接到正在运行的虚拟机。默认凭据就是用户用来登录当前 Windows 会话的凭据。选中“自动使用默认凭据(无提示)”复选框。

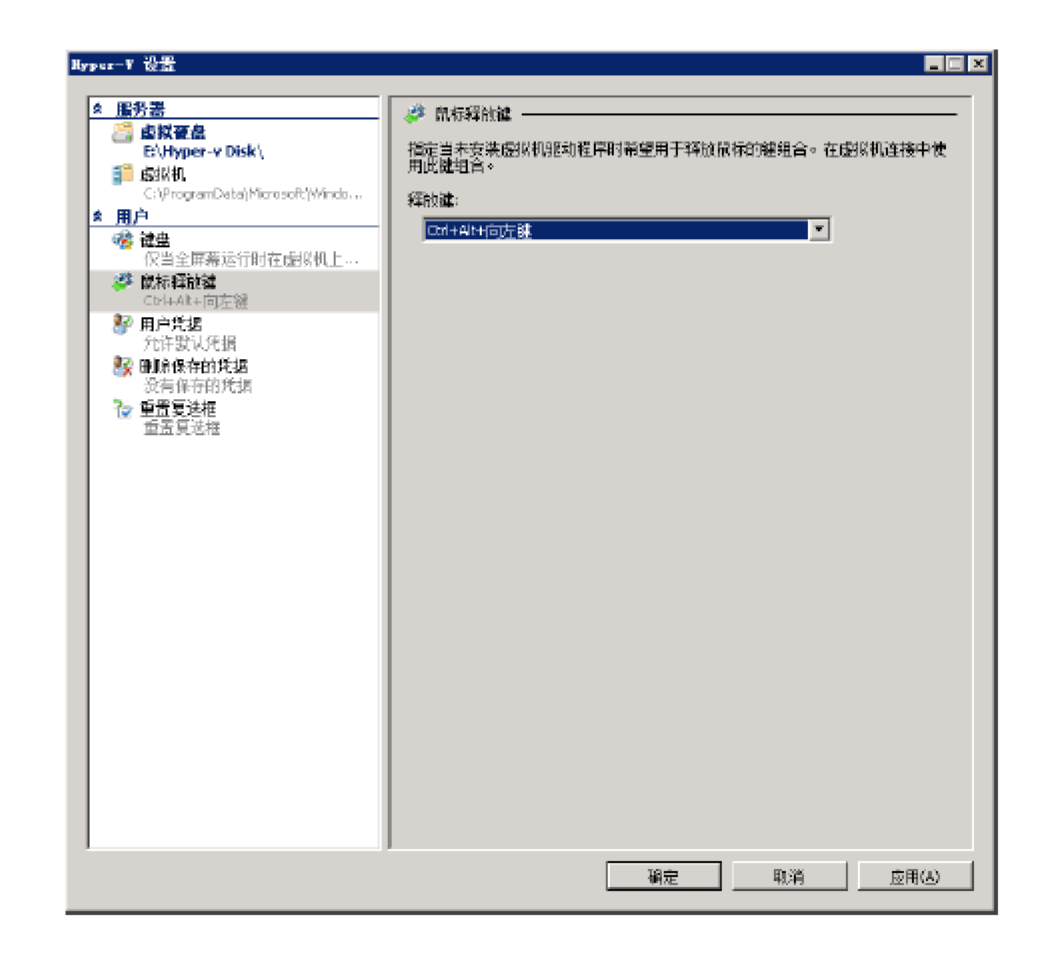


图 13-14　鼠标释放键

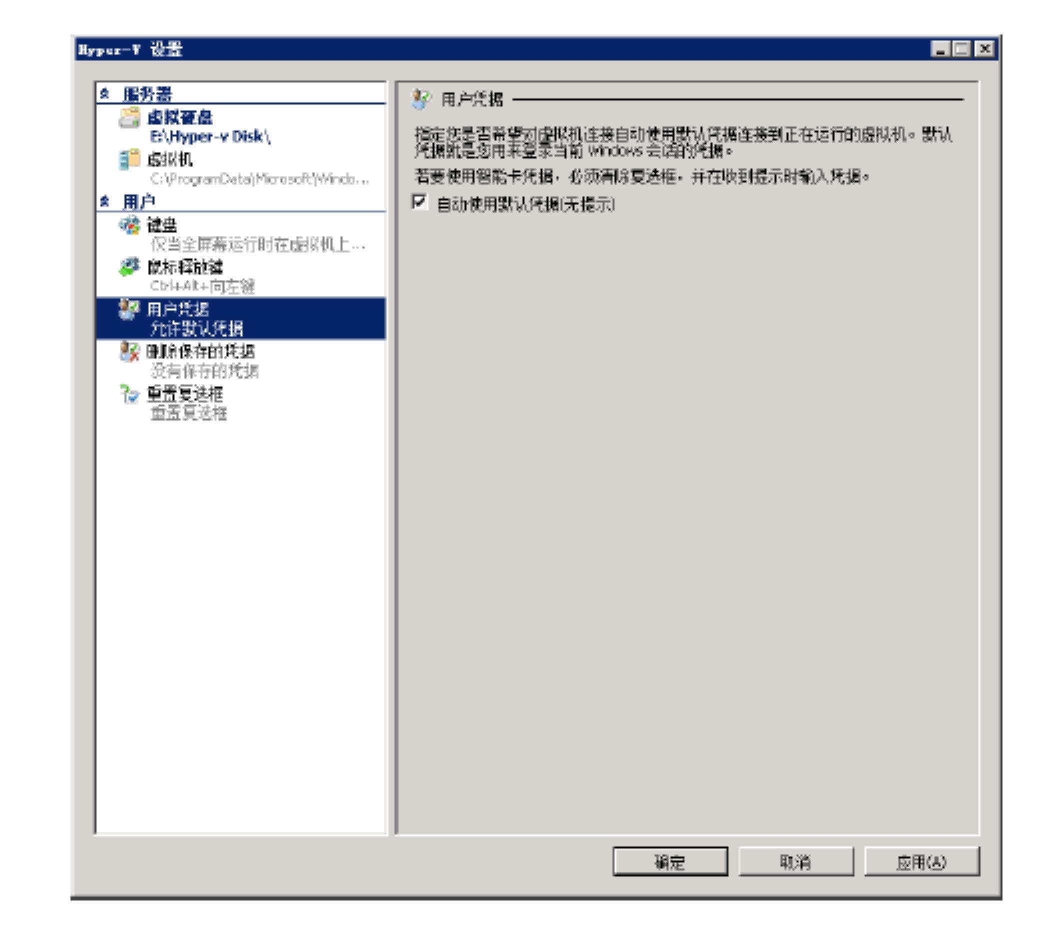


图 13-15　用户凭据

13.3.3　创建并安装虚拟机

① 选择“开始”→“程序”→“管理工具”→“Hyper-V 管理器”命令。

② 如图 13-16 所示，选择“新建”→“虚拟机”命令。

③ 如图 13-17 所示，在弹出的“开始之前”界面中，单击“下一步”按钮。

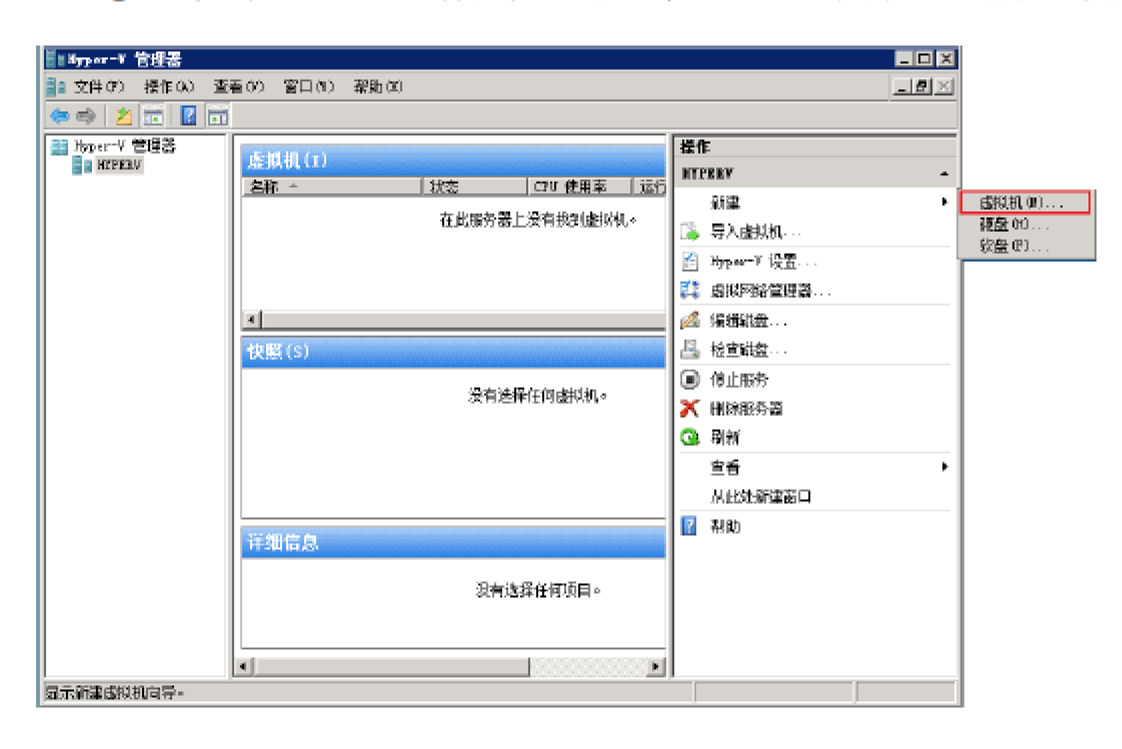


图 13-16　新建虚拟机



图 13-17　新建虚拟机向导

④ 如图 13-18 所示，在弹出的“指定名称和位置”界面中，输入名称，单击“下一步”按钮。

⑤ 如图 13-19 所示，在出现的“分配内存”界面中，输入虚拟机使用的内存，单击“下一步”按钮。

⑥ 如图 13-20 所示，在出现的“配置网络”界面中，按照图中所示选择连接，单击“下一步”按钮。

⑦ 如图 13-21 所示，在“连接虚拟硬盘”界面中，选中“创建虚拟硬盘”单选按钮，输入名称和大小以及位置，单击“下一步”按钮。

⑧ 如图 13-22 所示，在“安装选项”界面中，选中“从引导 CD/DVD-ROM 安装操作系统”单选按钮，并选中“映像文件”单选按钮，浏览到 Windows Server 2008 的安装文件，单击“下一步”按钮。

⑨ 如图 13-23 所示，在“正在完成新建虚拟机向导”界面中，选中“创建之后启动虚拟机”复选框，

单击“完成”按钮。

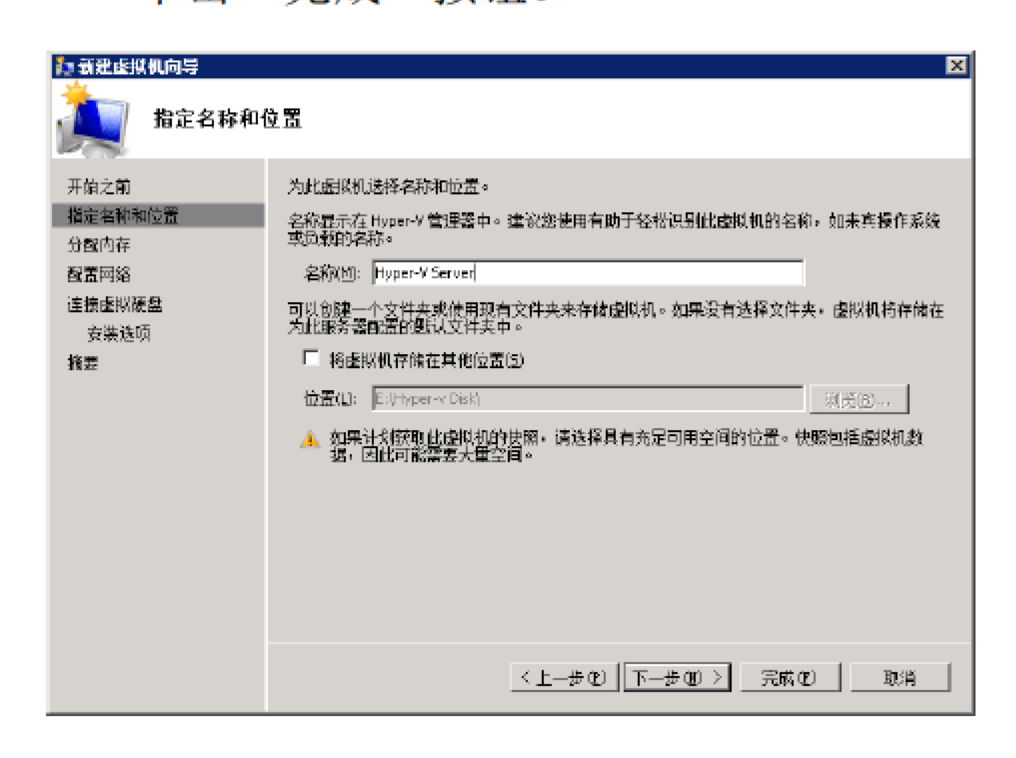


图 13-18 指定虚拟机名称和位置

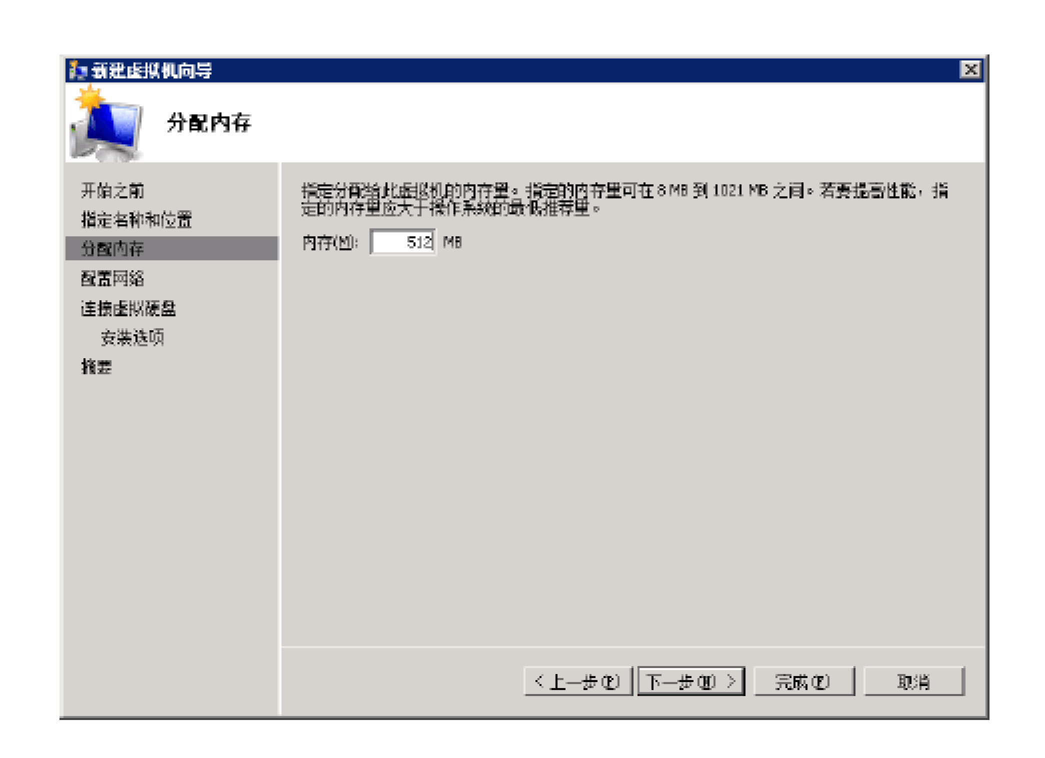


图 13-19 指定内存

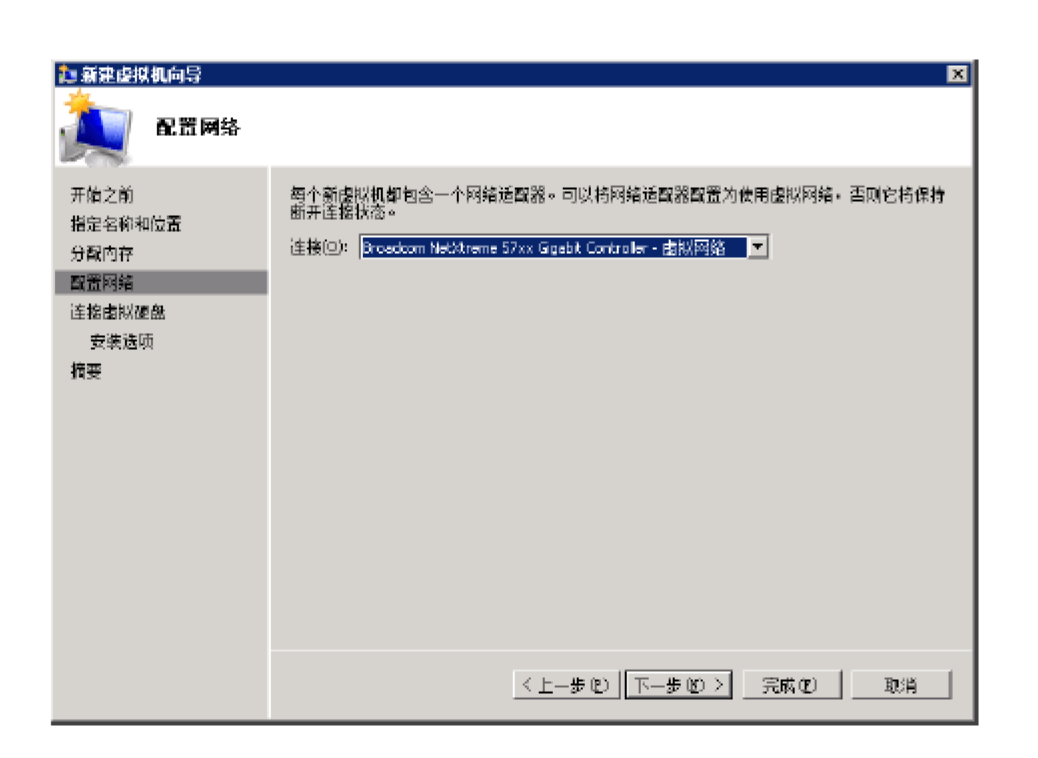


图 13-20 指定网络



图 13-21 创建虚拟硬盘



图 13-22 指定光驱



图 13-23 完成创建虚拟机向导

⑩ 完成 Windows Server 2008 64 位企业版的安装。

13.3.4 安装集成服务

用 Hyper-V 作了虚拟机以后，应安装 Integration Service。集成了驱动程序和其他一些虚拟机的增强程序，可以提高速度，也可以使你的鼠标自由出入虚拟机。但还是不支持文件拖入拖出，毕竟其目的是做

网络服务器使用，而不是演示操作。

在来宾操作系统安装集成服务

① 选择“开始”→“程序”→“管理工具”→“Hyper-V 管理器”命令。

② 如图 13-24 所示，右击安装好了的虚拟机，从弹出的快捷菜单中选择“连接”命令。

③ 如图 13-25 所示，在出现的虚拟机连接对话框中，选择“文件”→“设置”命令。

④ 如图 13-26 所示，在出现的设置对话框中，单击“集成服务”，可以看到集成服务包括的服务。

⑤ 如图 13-27 所示，选择“操作”→“插入集成服务安装盘”命令。

⑥ 在虚拟机中出现如图 13-28 所示的对话框，单击“安装 Hyper-V 集成服务”按钮。

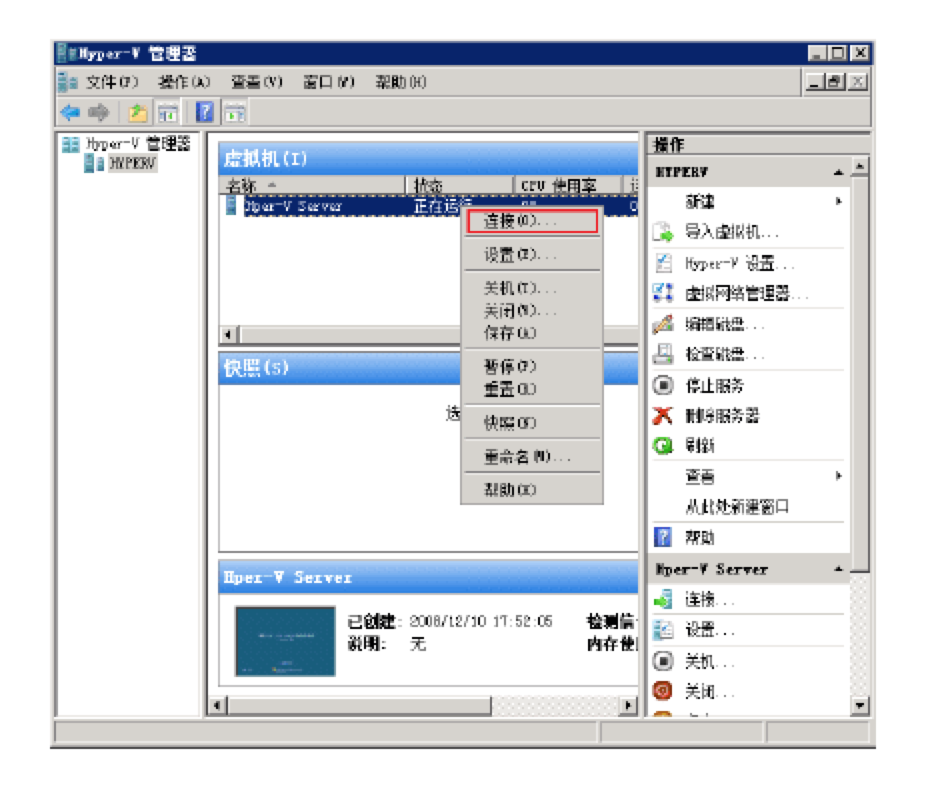


图 13-24 连接虚拟机

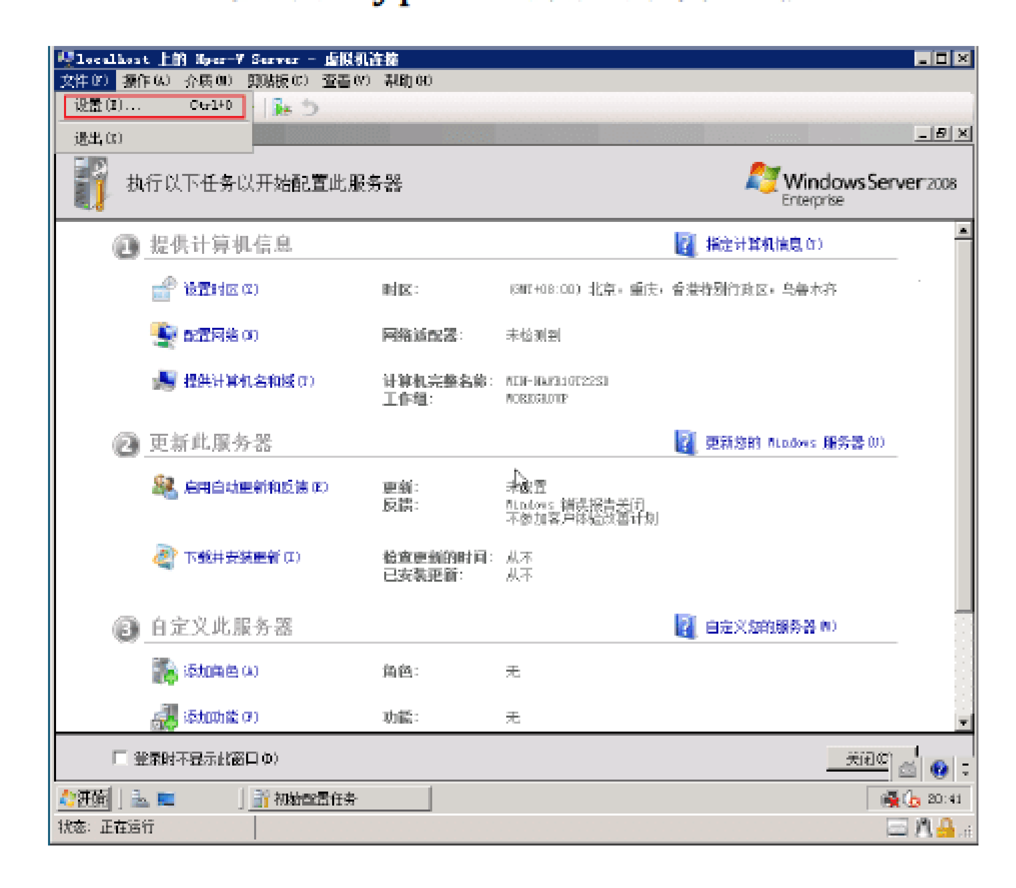


图 13-25 设置虚拟机

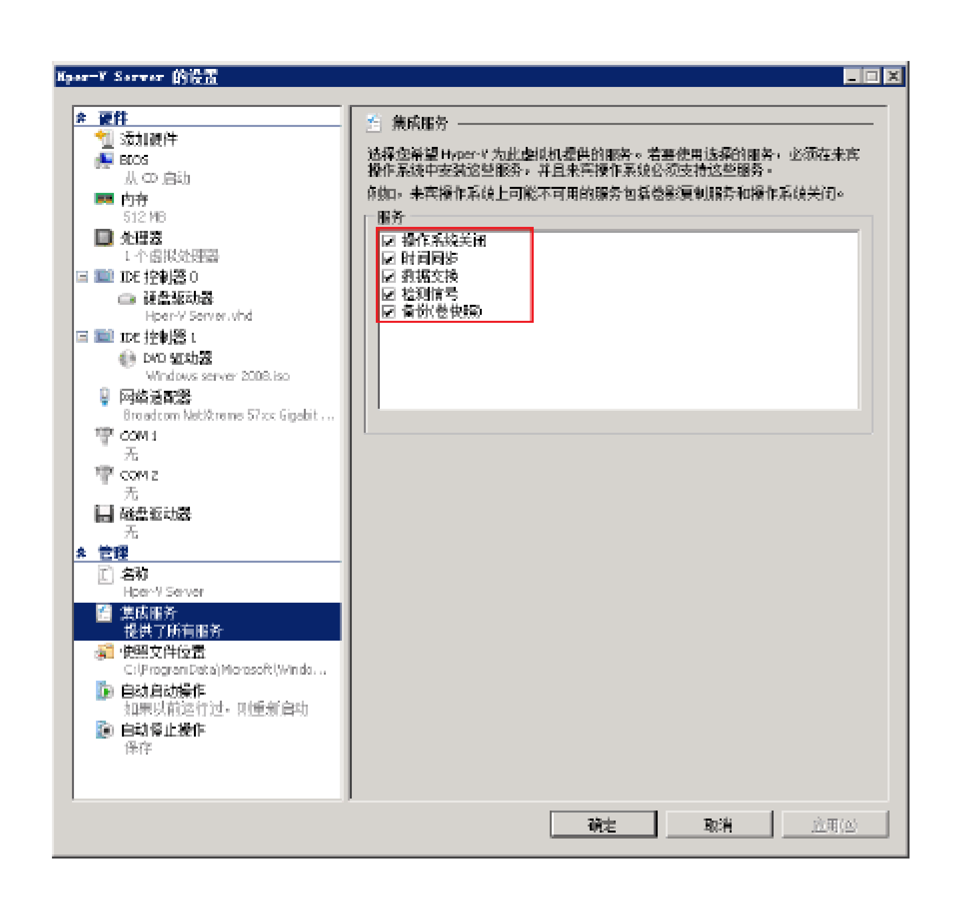


图 13-26 集成服务

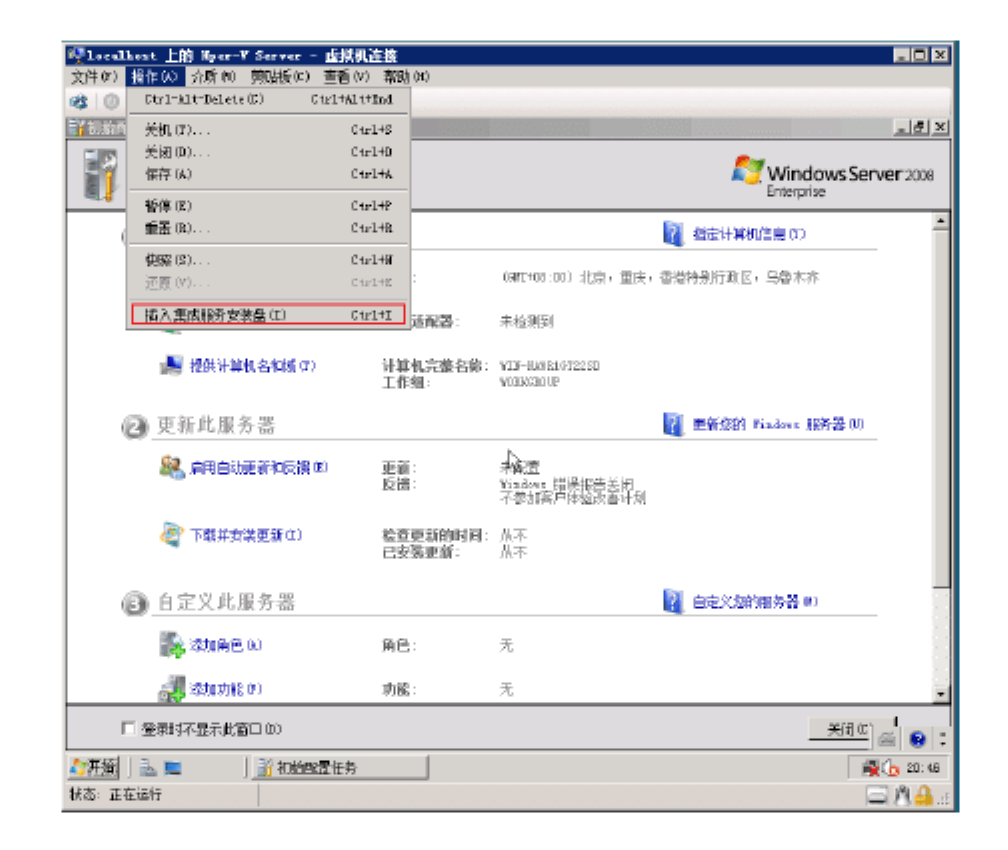


图 13-27 插入集成服务安装盘

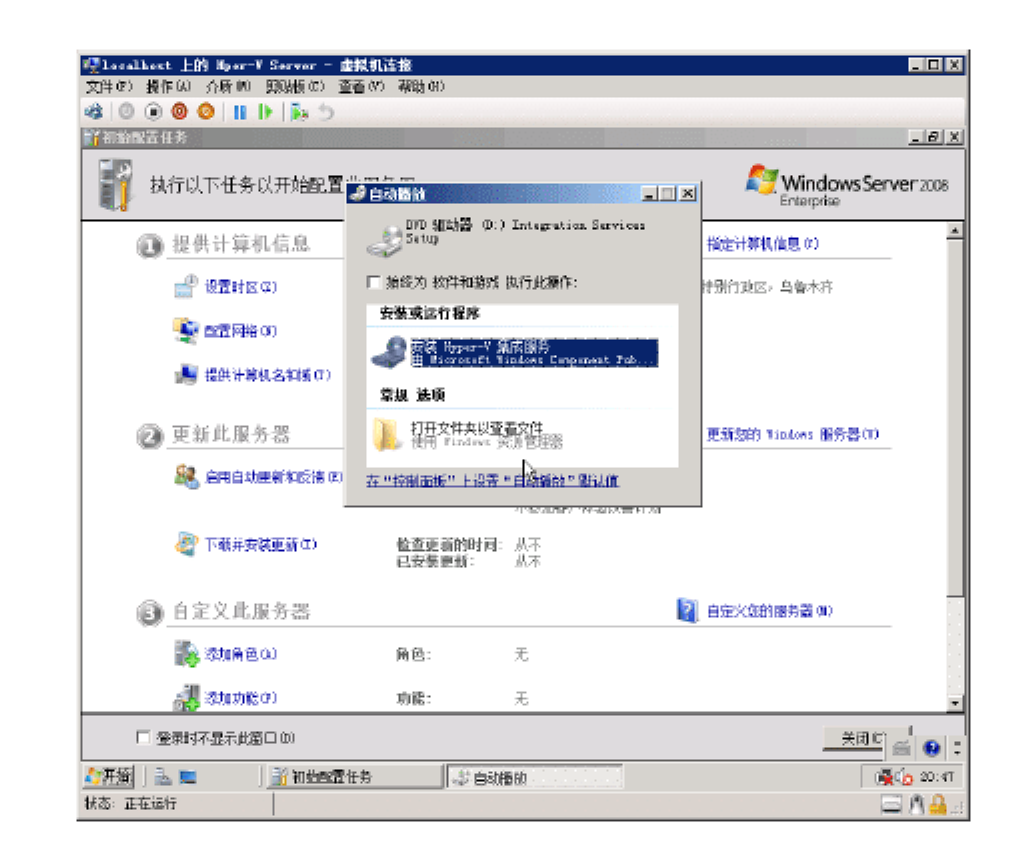


图 13-28 安装集成服务

⑦ 重启系统。

13.3.5 虚拟机设置

“虚拟机设置”为我们提供了一种创建虚拟机后调整虚拟机配置的方法。

① 如图 13-29 所示，打开虚拟机管理工具，选中虚拟机，单击“设置”按钮。

② 如图 13-30 所示，可以更改虚拟机的硬件以及内存 CPU 资源分配。

1. 硬件设置以及说明

- 内存：指定足够的内存，以运行来宾操作系统以及将在虚拟机上同时运行的所有程序。
- 虚拟处理器：如果虚拟机运行 Windows Server 2008 或 Windows Server 2003 作为来宾操作系统，则可以分配多个虚拟处理器。

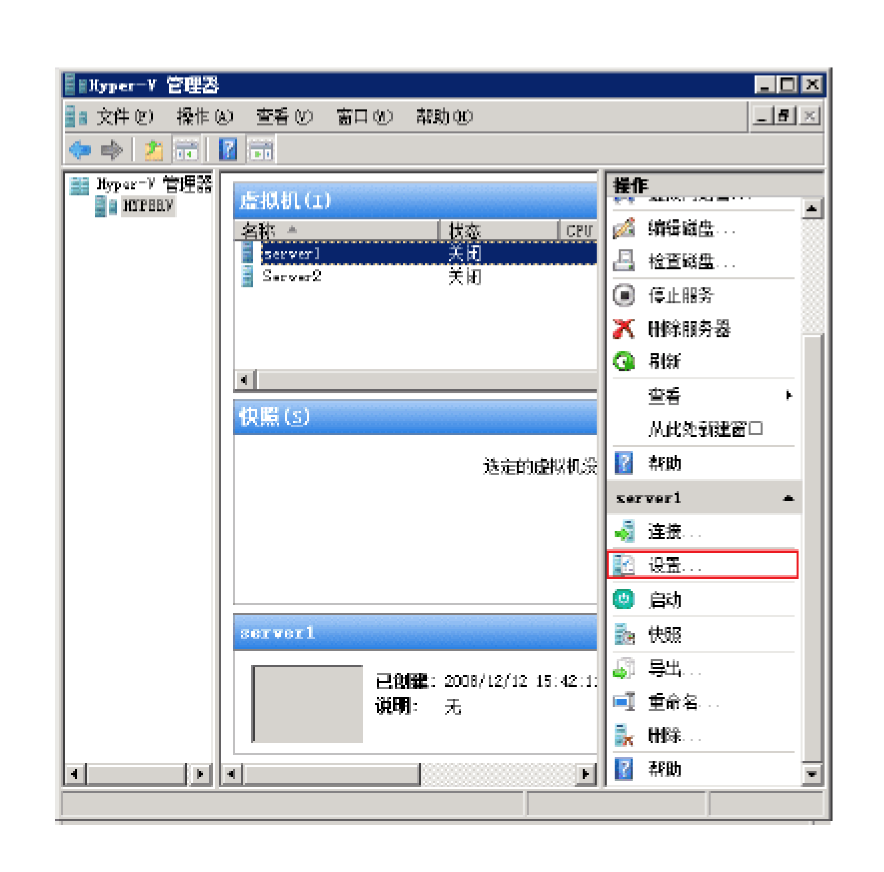


图 13-29 设置虚拟机

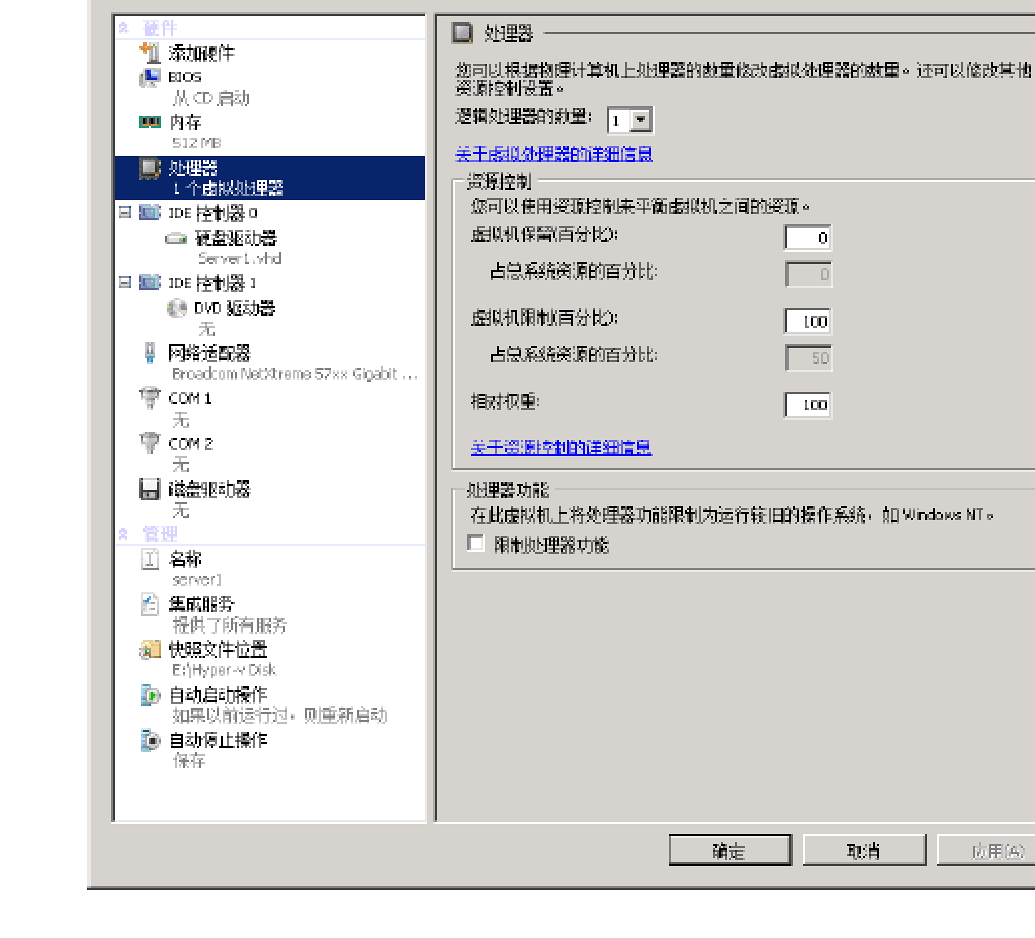


图 13-30 更改虚拟机设置

- 资源控制：这些设置为用户提供了一种控制如何在一个物理计算机上同时运行的虚拟机之间分配资源的方法。
- COM 编号：附加到命名管道的虚拟 COM 端口，经常和内核调试程序一起使用。

注意：无法将虚拟 COM 端口与物理 COM 端口关联。

- 软盘驱动器：软盘驱动器使虚拟机可以使用虚拟软盘。

注意：无法将软盘驱动器与物理软盘驱动器关联。

2. 管理设置以及说明

- 快照文件位置：该设置允许用户通过选择不同的位置替代默认位置。默认位置就是为运行 Hyper-V 的服务器指定的位置。
- 自动启动操作：这些设置允许用户指定如果物理计算机或 Hyper-V 虚拟机管理服务重新启动，是

否重新启动虚拟机。


注意： 如果计划使虚拟机高度可用，请不要将虚拟机配置为自动重新启动。

- 自动停止操作：这些设置允许用户指定当物理计算机关闭时希望虚拟机所处的状态。

13.3.6 创建和还原虚拟机快照

可不可以及时地返回到以前的某个时间点，然后看看当时你的虚拟机是怎样的？比如，在关键任务应用中安装预测产品补丁之前，你的虚拟机是怎样的？或者，由于在 SQL update 语句中遗漏了 where 语句，导致登录窗口的密码意外溢出之前，虚拟机又是如何？

幸好，微软的 Hyper-V 提供了一个很有用的工具，可以帮助用户创建和应用虚拟机的即时状态浏览：快照功能。这个工具很好用，可以从 Hyper-V 管理控制台创建虚拟机快照。

虚拟机一旦创建完毕即可创建快照。通常，快照的创建过程只有几秒钟，而且虚拟机不需暂停、停止或关闭。快照是由 Hyper-V 创建、执行的，它完全独立于运行在子分区的子操作系统的类型和性能。快照相关文件会自动储存到 Hyper-V 服务器设置的默认路径下。

在 Hyper-V 管理控制台可以轻松地创建快照，只需右击虚拟机，从弹出的快捷菜单中选择“快照”命令即可。任何时刻都可以创建快照，它会自动嵌入该虚拟机的即时状态浏览树结构中。在快照属性中，可以查看快照的详细信息。快照中储存的设置是只读的，除非将它们应用到现有虚拟机。

① 如图 13-31 所示，右击选中的虚拟机，从弹出的快捷菜单中选择“快照”命令，过一会儿，发现已经创建了虚拟机的快照。可以创建多个快照。

② 如图 13-32 所示，右击创建的快照，从弹出的快捷菜单中选择“应用”命令，还原到快照。

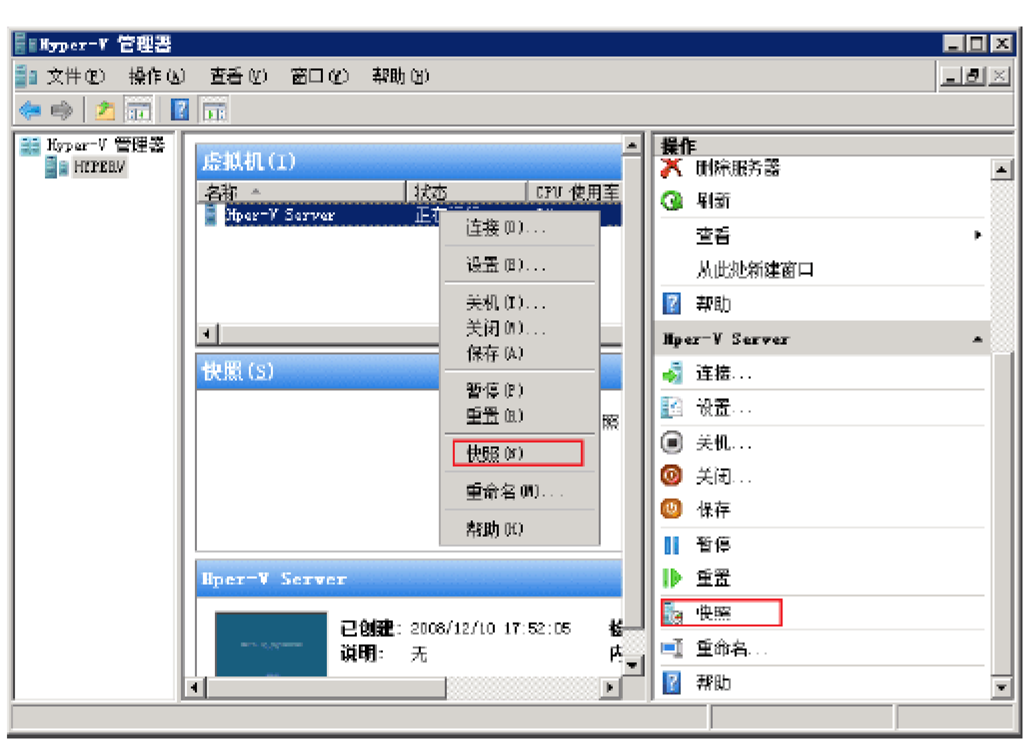


图 13-31 创建快照

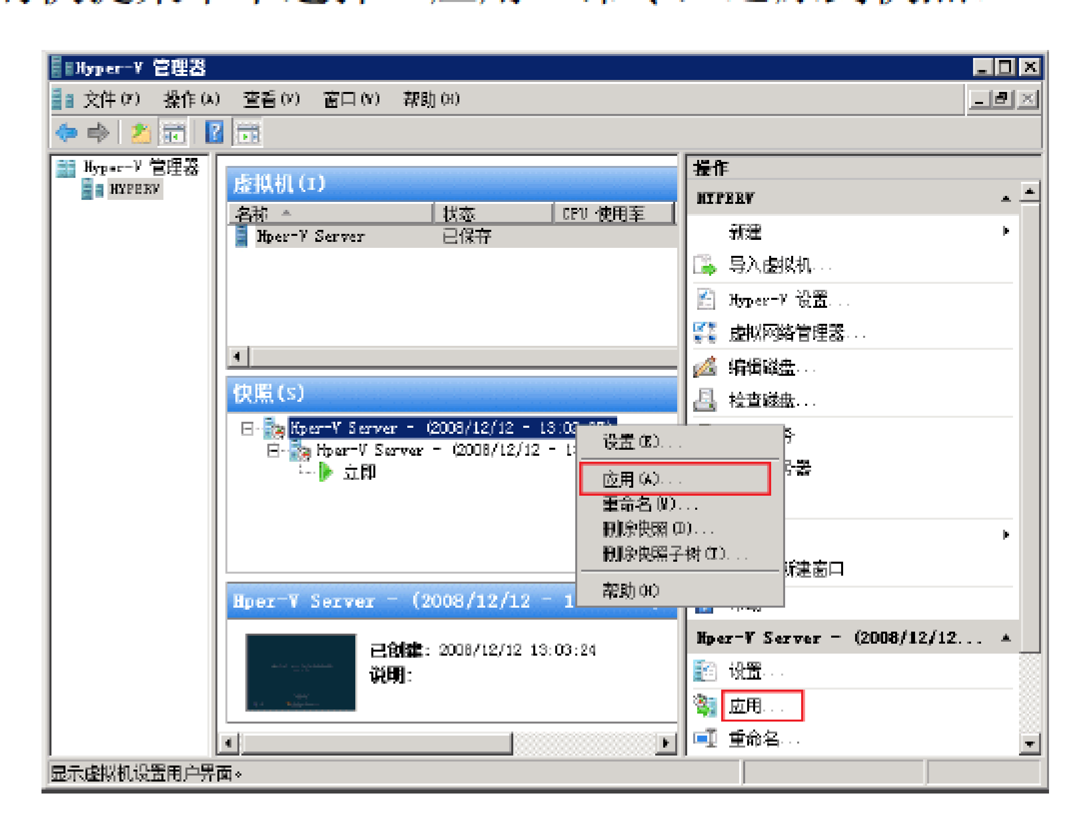


图 13-32 选择“应用”命令

③ 如图 13-33 所示，在出现的对话框中，单击“获取快照然后应用”按钮，系统就会将现在的状态立即创建快照，然后还原到选中的快照。

④ 如图 13-34 所示，可以看到系统当前的位置。使用快照，可以在虚拟机系统任何状态之间切换。

⑤ 如图 13-35 所示，右击快照，从弹出的快捷菜单中选择“删除快照子树”命令。

⑥ 如图 13-36 所示，可以看到删除了快照子树。



图 13-33　还原到快照前做快照

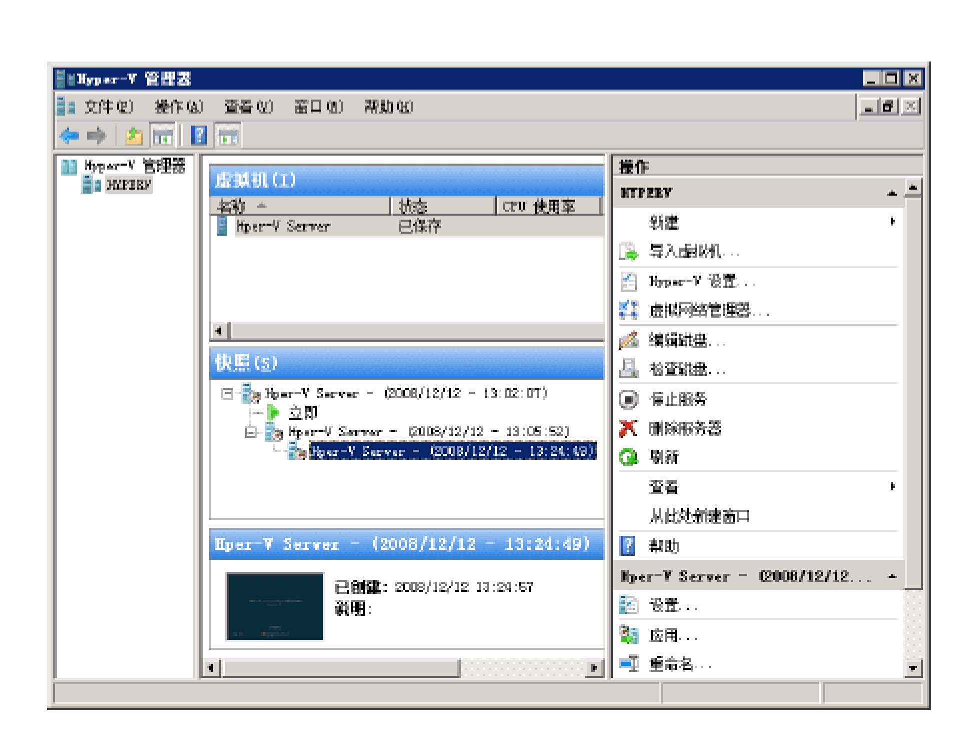


图 13-34　当前位置

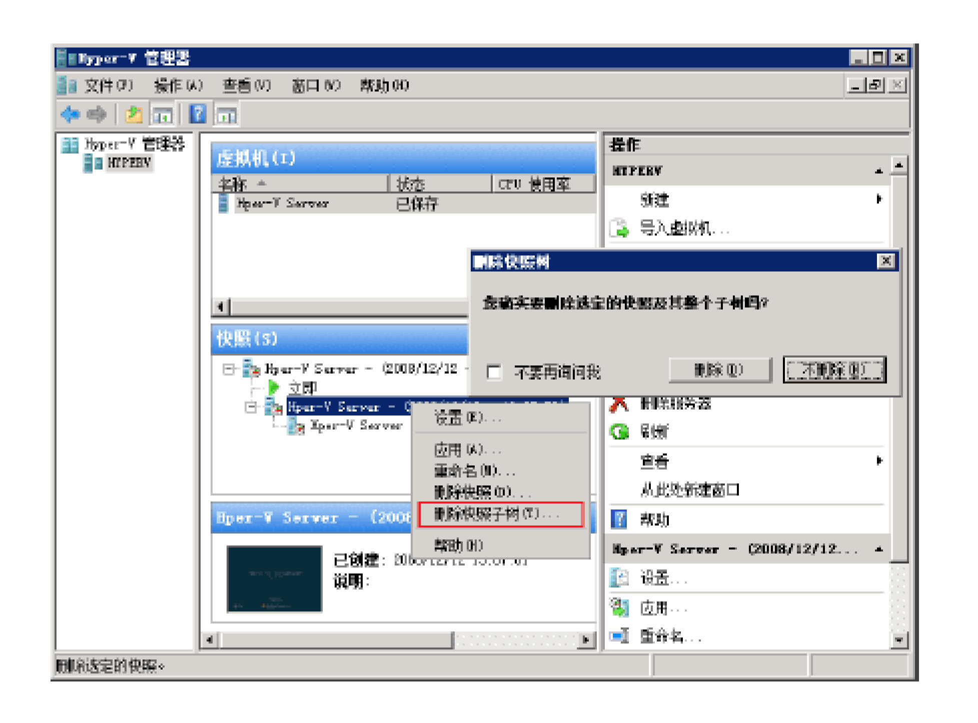


图 13-35　删除快照子树

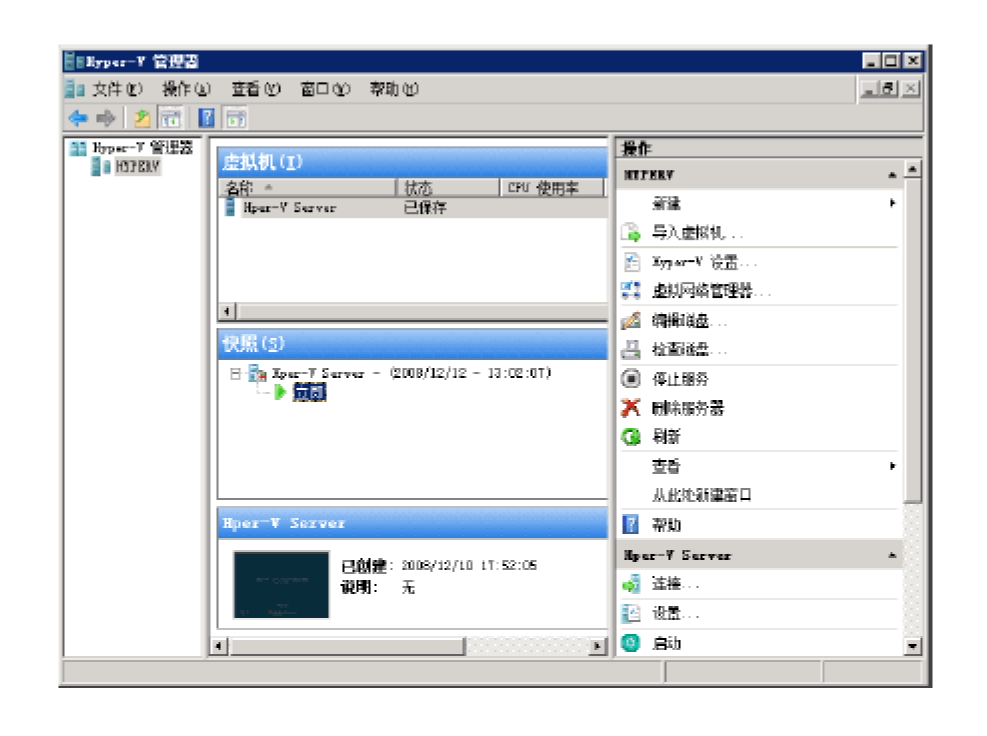


图 13-36　删除快照后

13.3.7　使用差异磁盘克隆系统

如何利用差异磁盘和 SYSPREP 功能设立多个 Windows Server 2008 的安装呢？

签于成本的原因，学习了解一项新的技术或是产品时，在没有部署到生产环境中之前，大家都会选择用虚拟机来搭建一套实验环境。但如何快速搭建呢？如何节省磁盘空间呢？

说到此不得不说一下 Hyper-V 的差异磁盘技术，这种方法就是先建立好一个虚拟机系统(GUEST OS)，并进行相关的设置，如桌面等，然后以此系统为模板(严格来说是此虚拟机系统安装后的硬盘为母盘)建立差异磁盘，并将此差异磁盘指派给新的虚拟机来使用。当用户使用新的虚拟机后，它仍会以母盘内的 Windows 2008 来启动系统，但是此后在此系统内所进行的任何变动都会被保存在差异磁盘内，而不会改变母盘内的内容。这样创建新的系统不但快捷，而且节省了磁盘空间。

差异磁盘技术在节省硬盘空间的同时，却带来了一个问题，由于依据母盘新派生出来的系统都具有同样的 SID，这将会给实验环境带来问题。可喜的是，Windows 2008 安装后就在系统中自带了 SYSPREP 工具(也可以使用 NEWSID.EXE 工具)，通过此更改新派生出来的系统的 SID，让这些问题不再成为问题。

使用已有系统克隆多个系统

① 选择“开始”→“程序”→“管理工具”→“Hyper-V 管理器”命令。

② 如图 13-37 所示，右击已经关闭的虚拟机，从弹出的快捷菜单中选择“删除”命令。这并不删除虚拟机的硬盘文件。

③ 如图 13-38 所示，选择“新建”→“硬盘”命令。

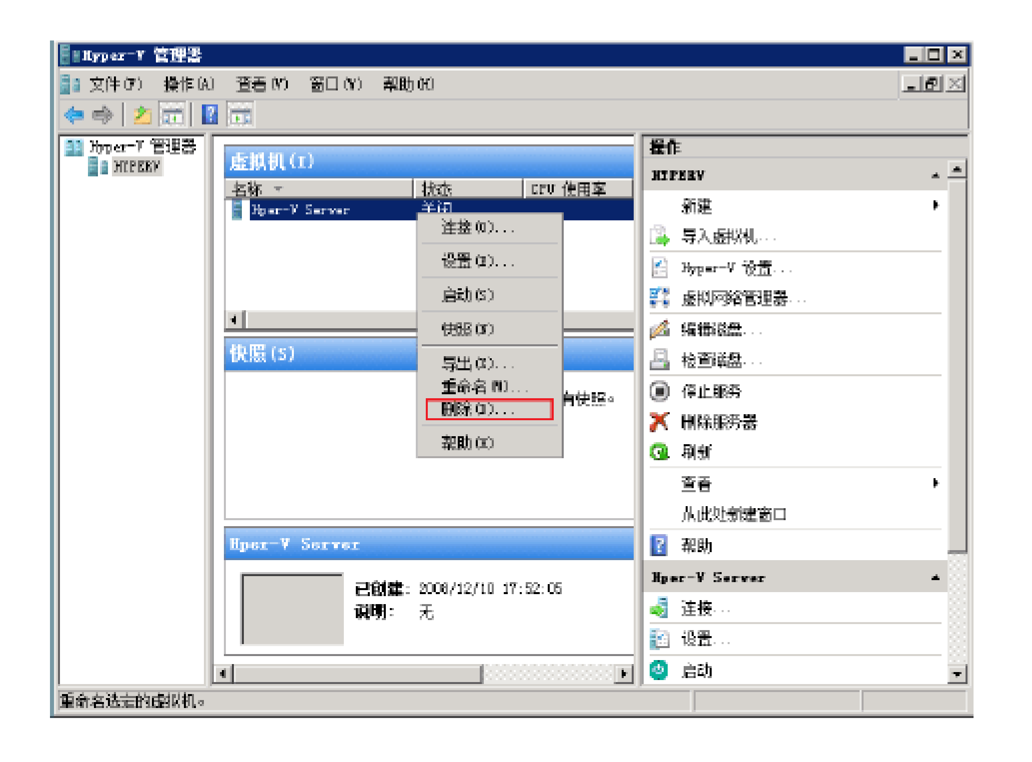


图 13-37 删除虚拟机



图 13-38 创建硬盘

④ 如图 13-39 所示，在出现的“开始之前”界面中，单击“下一步”按钮。

⑤ 如图 13-40 所示，在出现的“选择磁盘类型”界面中，选中“差异”单选按钮，单击“下一步”按钮。



图 13-39 创建磁盘向导

图 13-40 创建差异磁盘

⑥ 如图 13-41 所示，在“指定名称和位置”界面中，输入名称和位置，单击“下一步”按钮。

⑦ 如图 13-42 所示，在“配置磁盘”界面中，指定父硬盘的虚拟硬盘，单击“下一步”按钮，完成差异磁盘的创建。



图 13-41 指定磁盘位置和名称



图 13-42 指定父盘

⑧ 以同样的方法创建 Server2.vhd 差异磁盘。

⑨ 如图 13-43 所示，创建虚拟机 Server1 使用现有磁盘 Server1.vhd。

⑩ 如图 13-44 所示，创建虚拟机 Server2 使用现有磁盘 Server2.vhd。

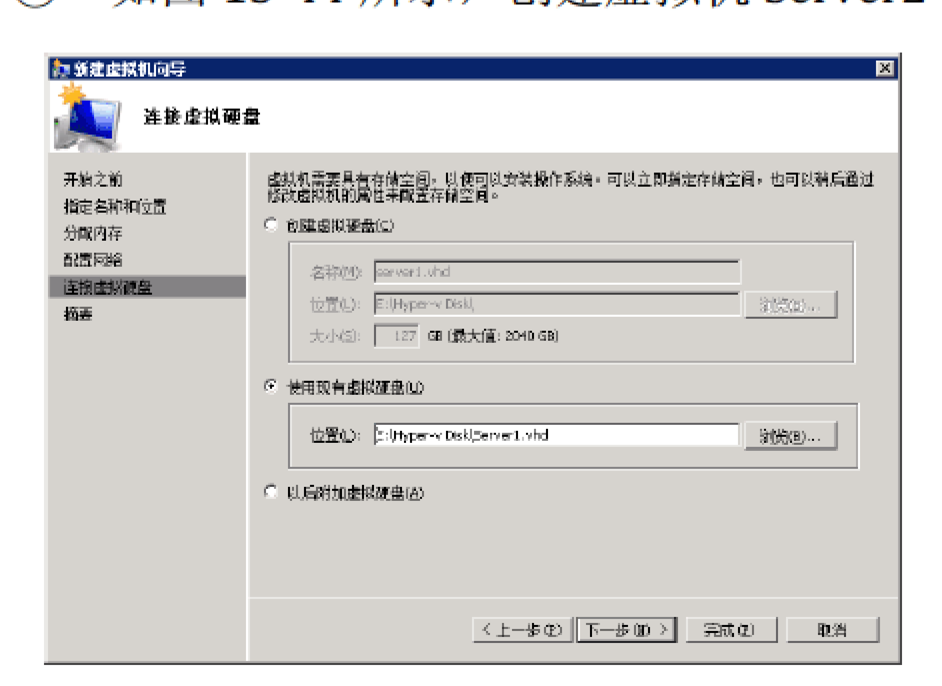


图 13-43 使用现有磁盘 Server1

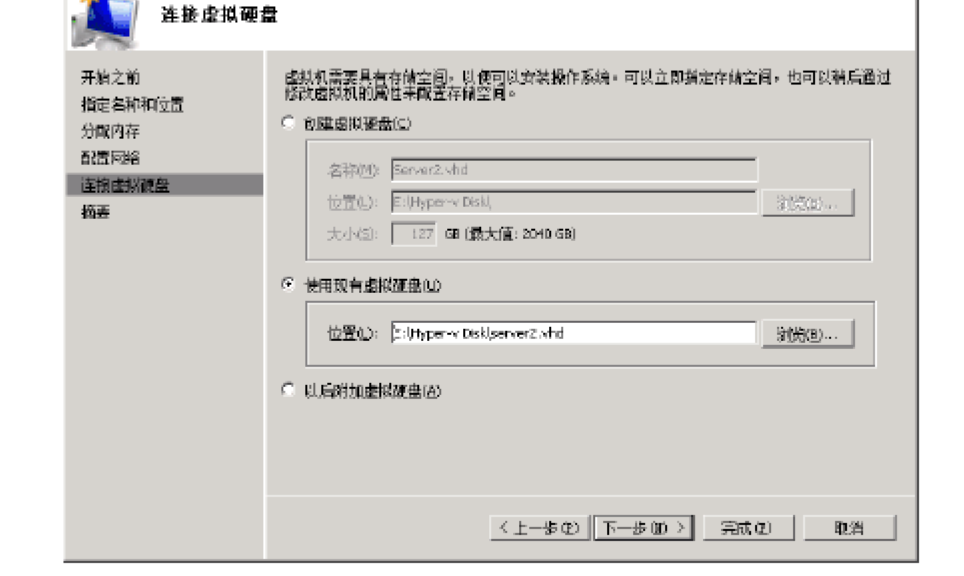


图 13-44 使用现有磁盘 Server2

⑪ 如图 13-45 所示，两个虚拟机启动后运行 sysprep。双击 sysprep，在出现的对话框中，选中“通用”复选框，单击“确定”按钮。

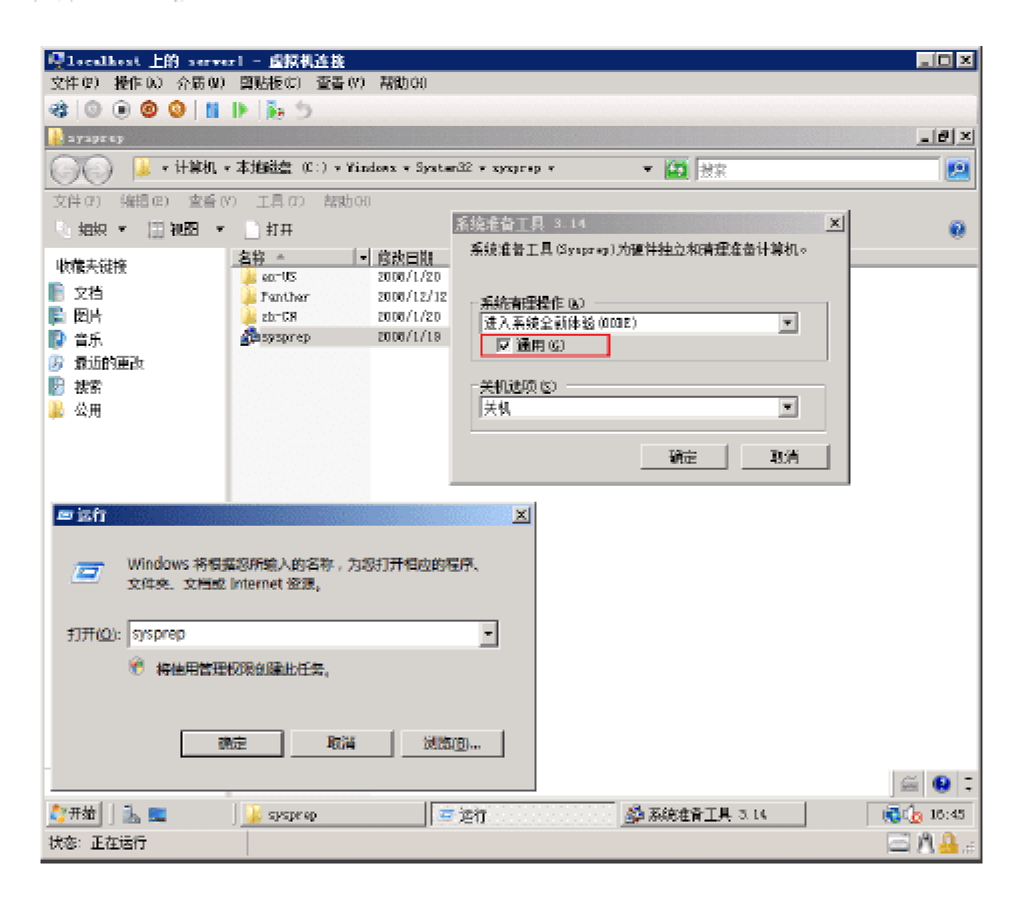


图 13-45 去掉计算机的 SID

⑫ 重启后，重新激活系统。

13.4 管理虚拟网络

可以在运行 Hyper-V 的服务器上创建许多虚拟网络以提供各种通信通道。例如，可以创建网络以提供以下通信通道。

- 仅虚拟机之间的通信。这种类型的虚拟网络称为专用网络。
- 虚拟化服务器和虚拟机之间的通信。这种类型的虚拟网络称为内部网络。
- 虚拟机和物理网络之间的通信，方法是创建与虚拟化服务器上物理网络适配器的关联。这种类型的虚拟网络称为外部网络。

可以使用虚拟网络管理器添加、删除和修改虚拟网络。虚拟网络管理器可以从 Hyper-V 管理器获得。

注意：如果将虚拟网络连接到使用静态设置(如静态 IP 地址)的物理网络适配器，并且未禁用 IPv6，则新连接将覆盖静态设置。在将静态设置重新应用于物理网络适配器之前，将丢失网络连接。

如图 13-46 所示，打开装有 Hyper-V 角色的物理机的网络连接，可以看到安装完 Hyper-V 后网络连接的变化，原来的网卡出现的本地连接，已经不再绑定 TCP/IP 协议，只绑定了 Microsoft 虚拟网络交换机协议，虚出来一个本地连接 3。物理机使用该连接的 IP 地址和网络中的其他计算机通信。

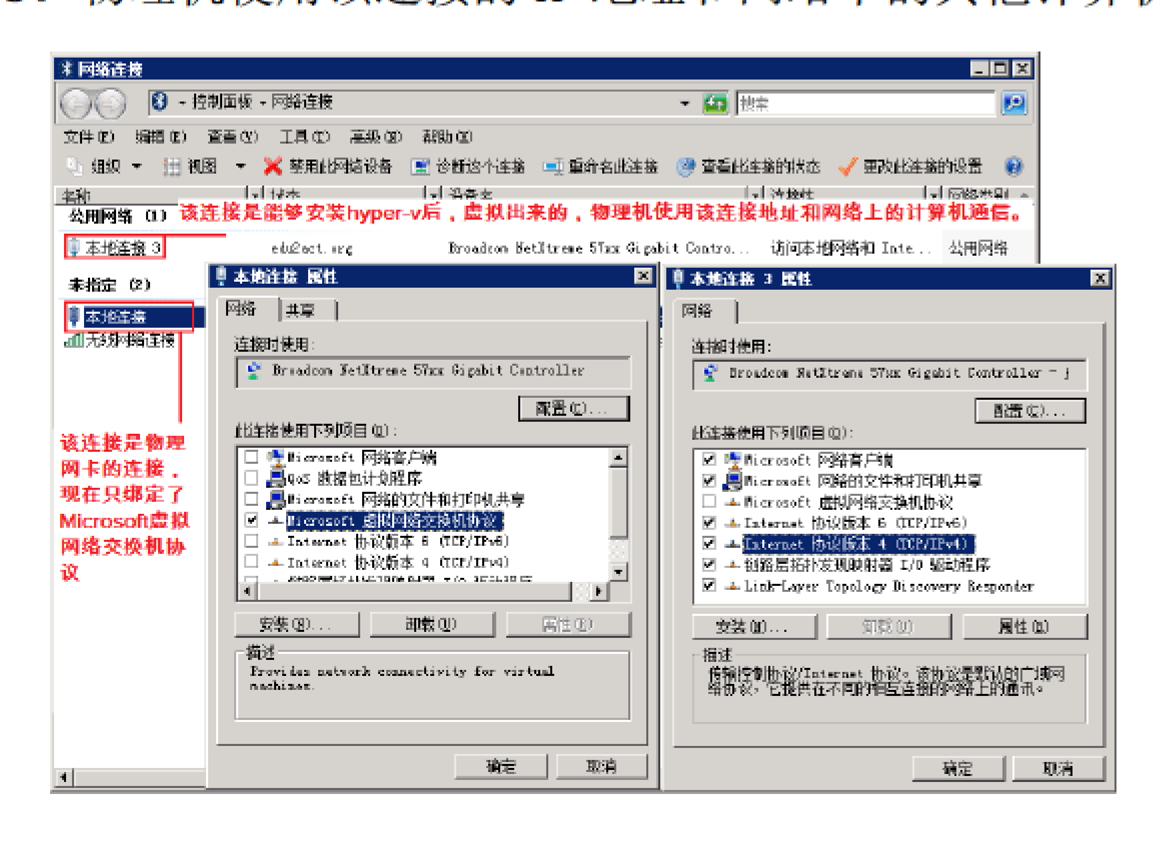


图 13-46　虚拟机网络和物理机网络

13.4.1　示例 1：创建和使用内部网络

1. 实验目标

以下将创建内部网络实现虚拟机和物理机通信，如图 13-47 所示。

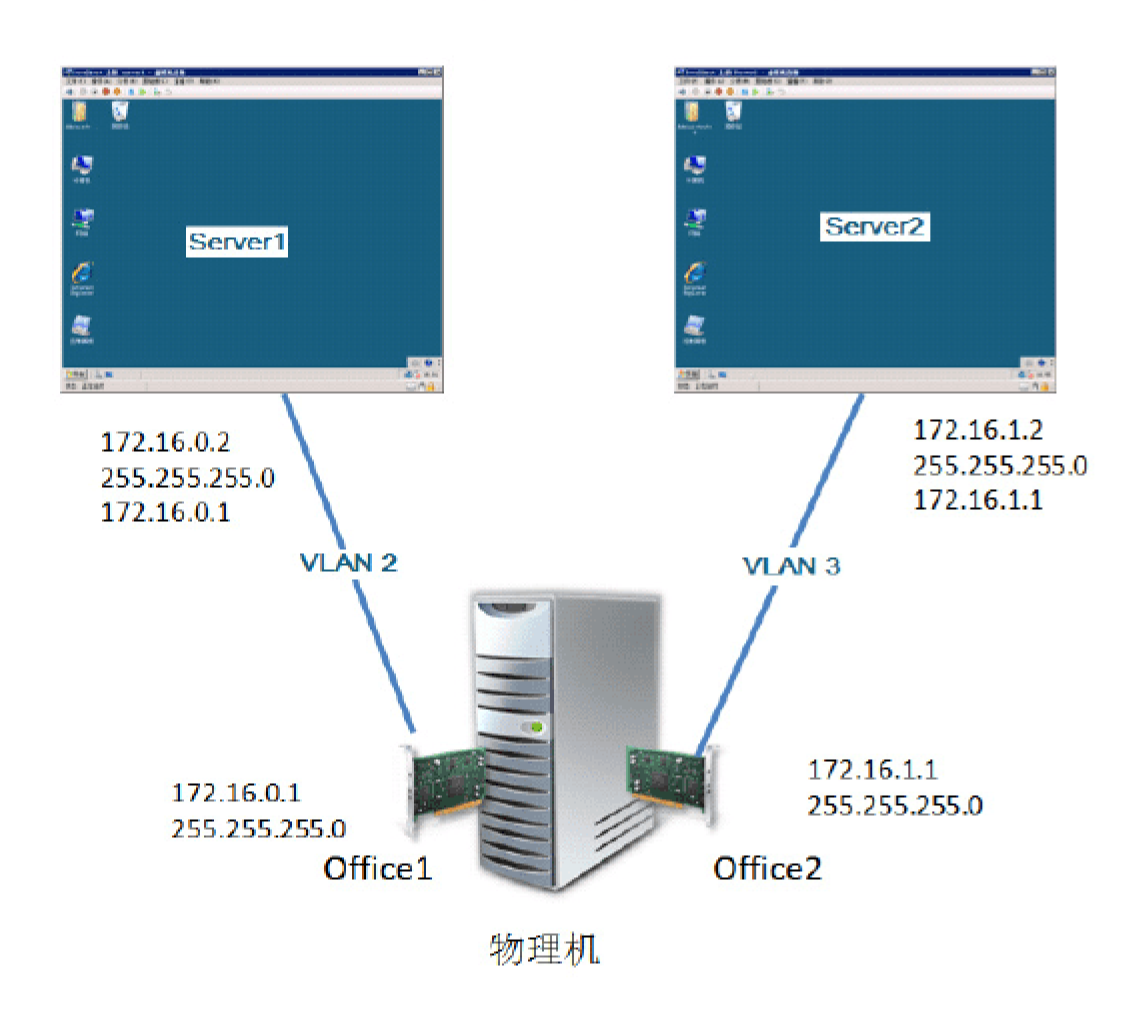


图 13-47　内部网络示意图

- 虚拟机 Server1 需要和物理机通信，使用 172.16.0.2、255.255.255.0 网段，将其放到 VLAN 2 中，IP 地址分配如图 13-47 所示。
- 虚拟机 Server2 需要和物理机通信，使用 172.16.1.2、255.255.255.0 网段，将其放到 VLAN 3 中，

IP 地址分配如图 13-47 所示。

■ 完成配置后 Server1 能够与物理机虚拟出来的网络连接 Office1 的 IP 地址通信，Server2 能够与物理机虚拟出来的网络连接 Office2 的 IP 地址通信。

注意：使用不同的 VLAN 编号可以从数据链路层隔离网络，隔绝网络广播。

2. 实验步骤

① 打开物理机的本地连接，如图 13-48 所示，注意观察网络连接的数量和名称。

② 如图 13-49 所示，打开 Hyper-V 管理工具，单击“虚拟网络管理器”按钮。

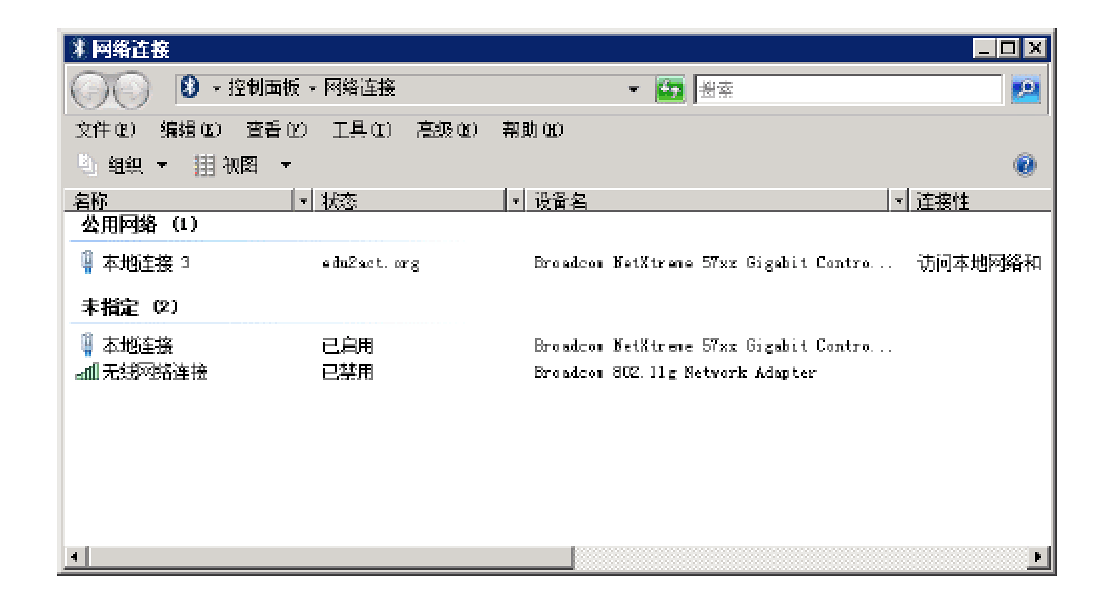


图 13-48　物理机的网络连接



图 13-49　管理虚拟网络

③ 如图 13-50 所示，在打开的“虚拟网络管理器”窗口，选择“新建虚拟网络”，网络类型选择“内部”，单击“添加”按钮。

④ 如图 13-51 所示，输入虚拟网络名称 Office1，选中“启用父分区的虚拟 LAN 标识”复选框，在下面的文本框中输入 2，单击“应用”按钮。

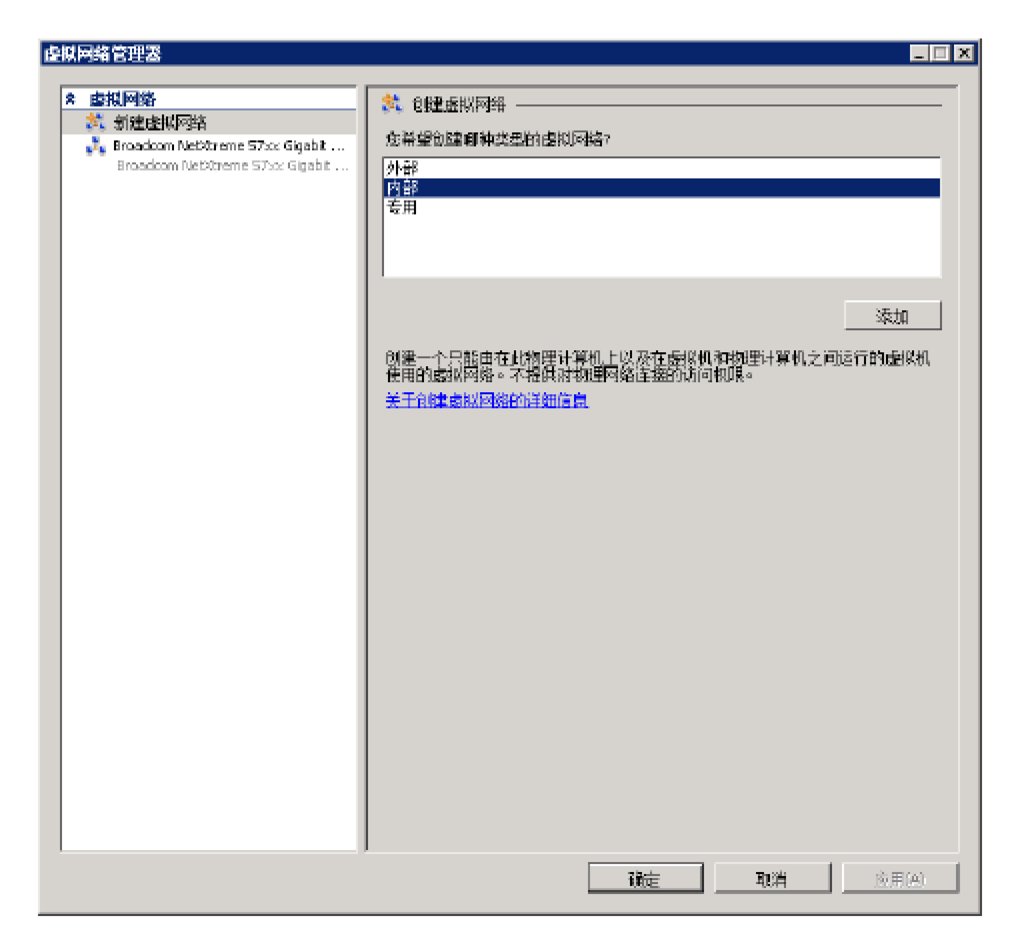


图 13-50　添加网络

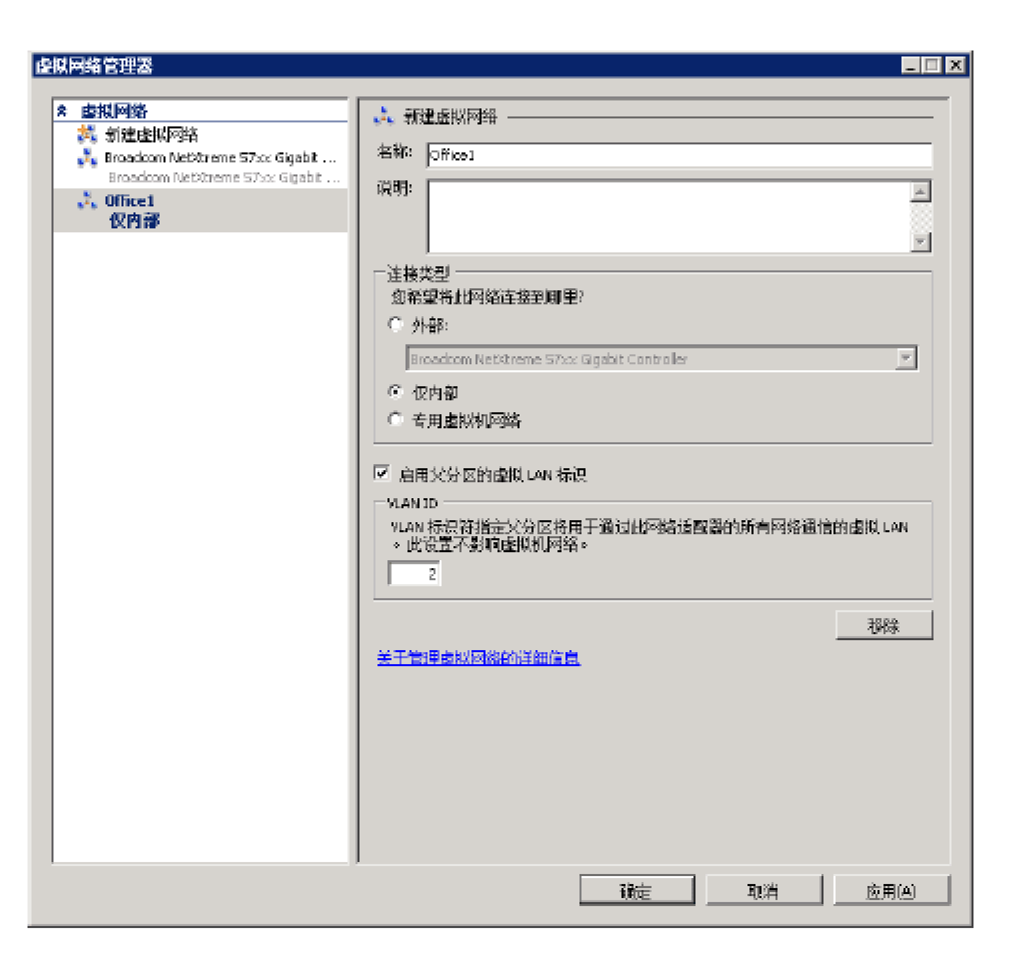


图 13-51　输入虚拟网络名称和 VLAN ID

⑤ 如图 13-52 所示，再次打开“虚拟网络管理器”对话框，选择“新建虚拟网络”，网络类型选择“内部”，单击“添加”按钮。

⑥ 如图 13-53 所示，输入新建网络的名称 Office2，选中“启用父分区的虚拟 LAN 标识”复选框，在下面的文本框中输入 3，单击“应用”按钮。

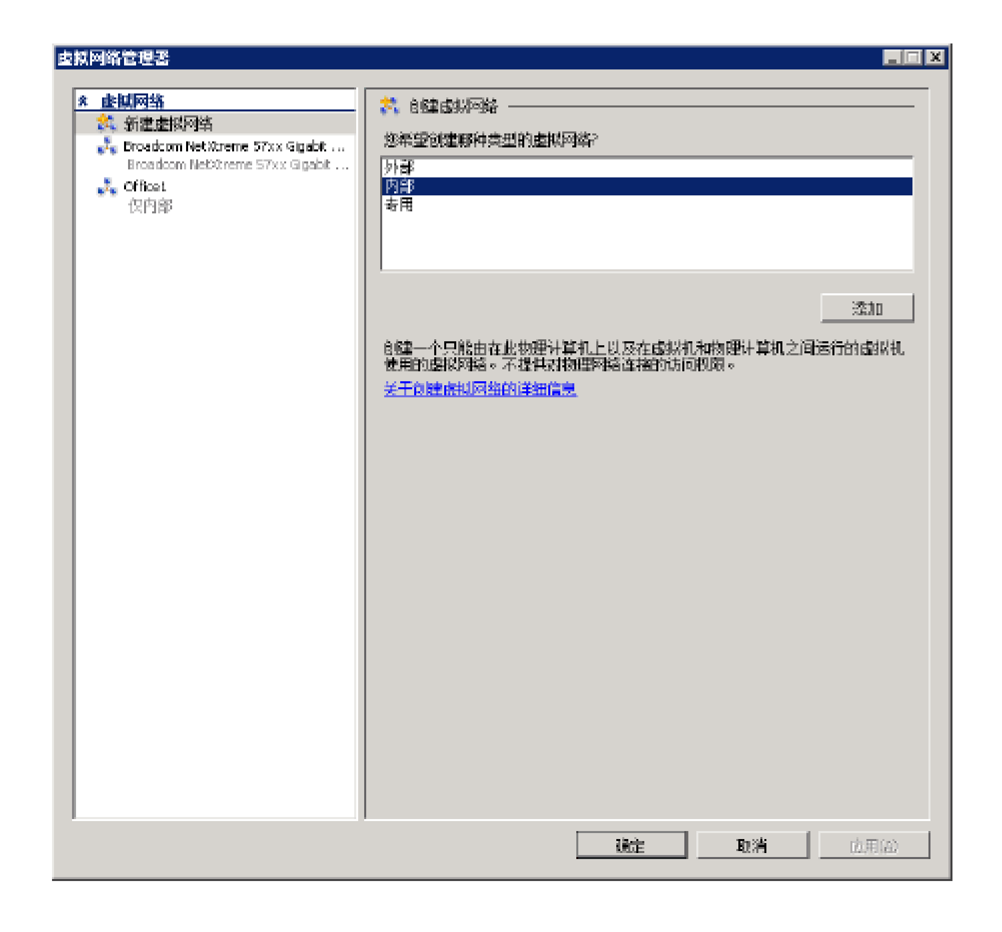


图 13-52　添加网络

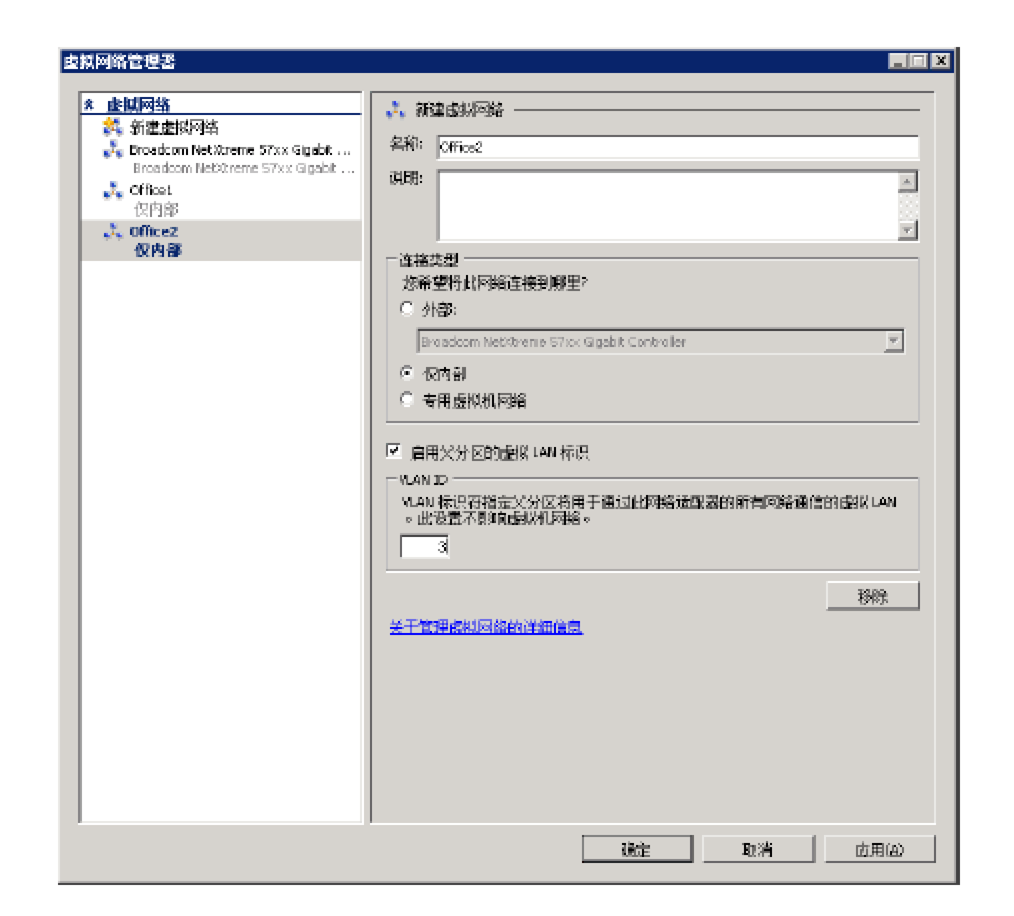


图 13-53　输入虚拟网络名称和 VLAN ID

⑦　如图 13-54 所示，打开物理机的网络连接，可以看到多出来 Office1 和 Office2 两个网络设备，如图中所示指定 Office1 和 Office2 的 IP 地址。

⑧　单击打开 Server1，如图 13-54 所示，选择“文件”→“设置”命令。

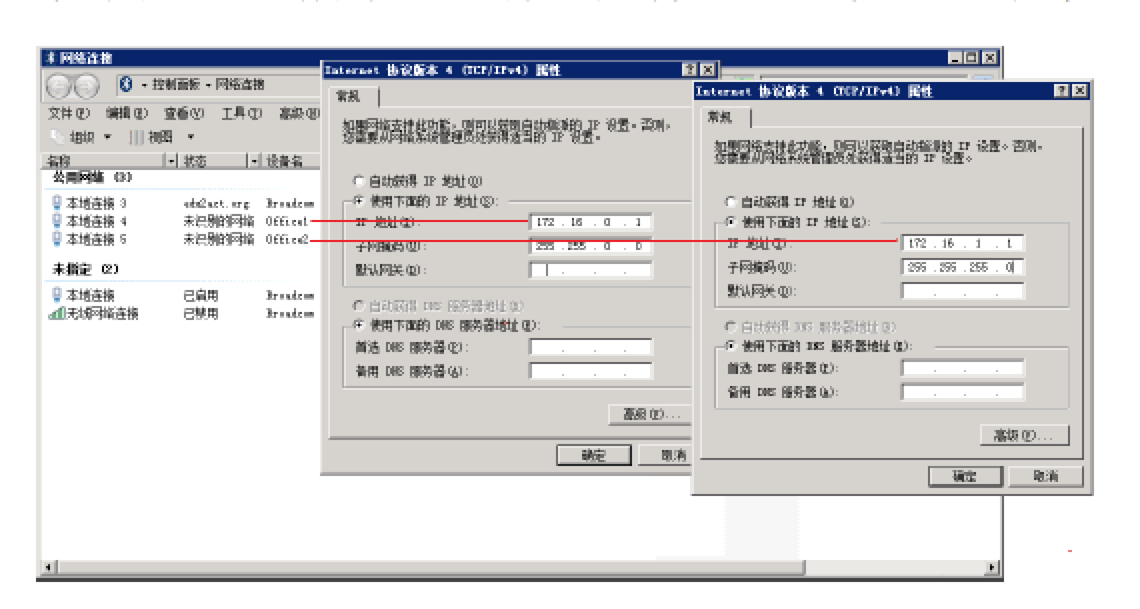


图 13-54　物理机的网络连接增加

⑨　如图 13-55 所示，在出现的“Server1 的设置”对话框中，选择“网络适配器”，网络选择 Office1，选中“启用虚拟 LAN 标识”复选框，在下面的文本框中输入 2，单击“确定”按钮。

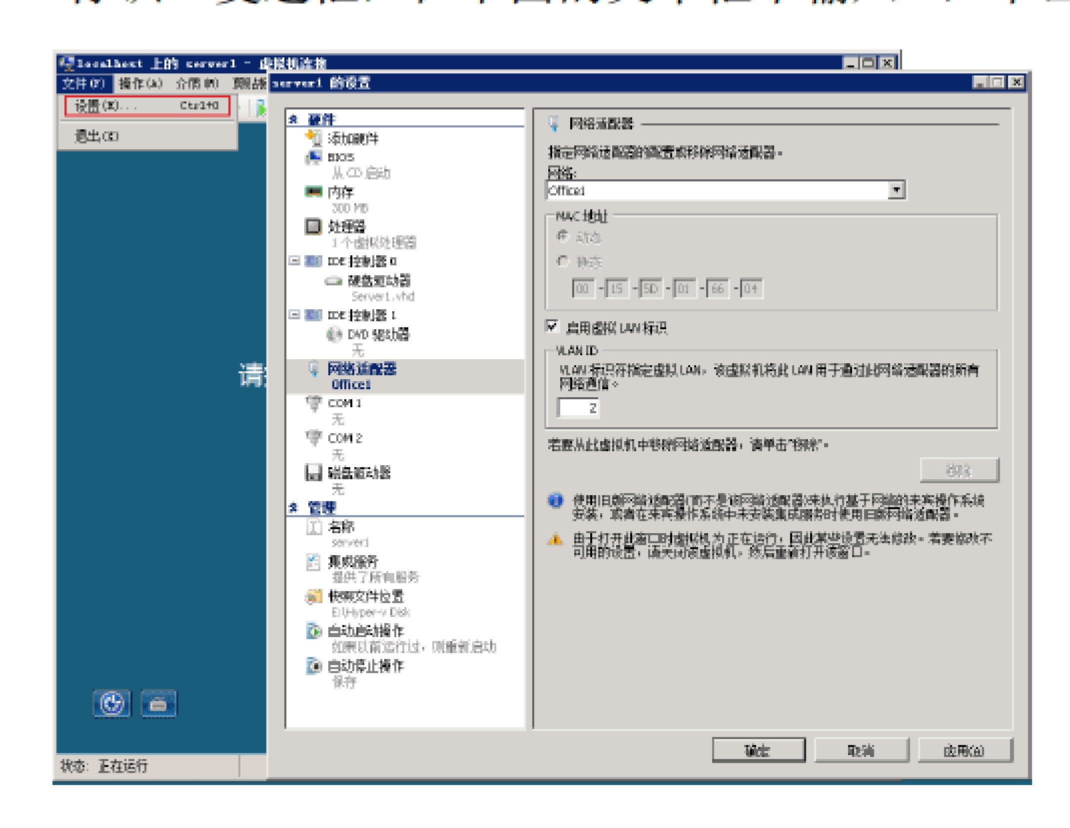
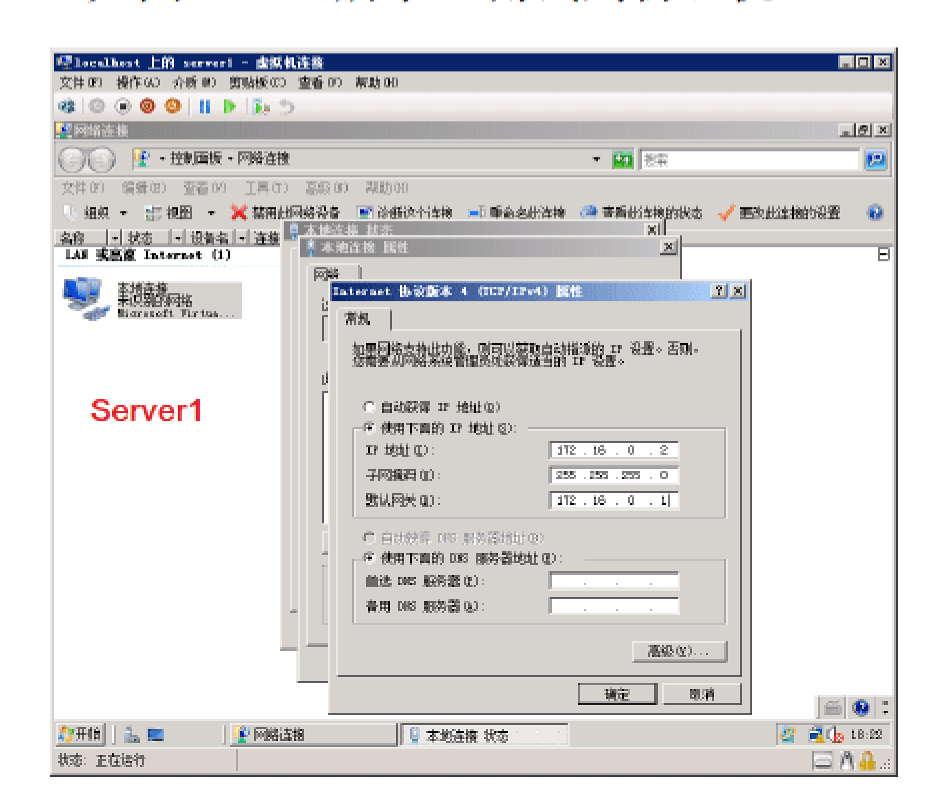
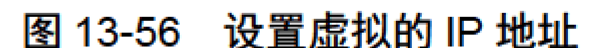


图 13-55　更改虚拟机使用的网络

⑩　如图 13-56 所示，设置 Server1 的 IP 地址为 172.16.0.2，子网掩码 255.255.255.0，网关 172.16.0.1。

⑪　如图 13-57 所示，测试到物理机 Office1 的连接，ping 172.16.0.1 发现是通的。




图 13-56　设置虚拟的 IP 地址

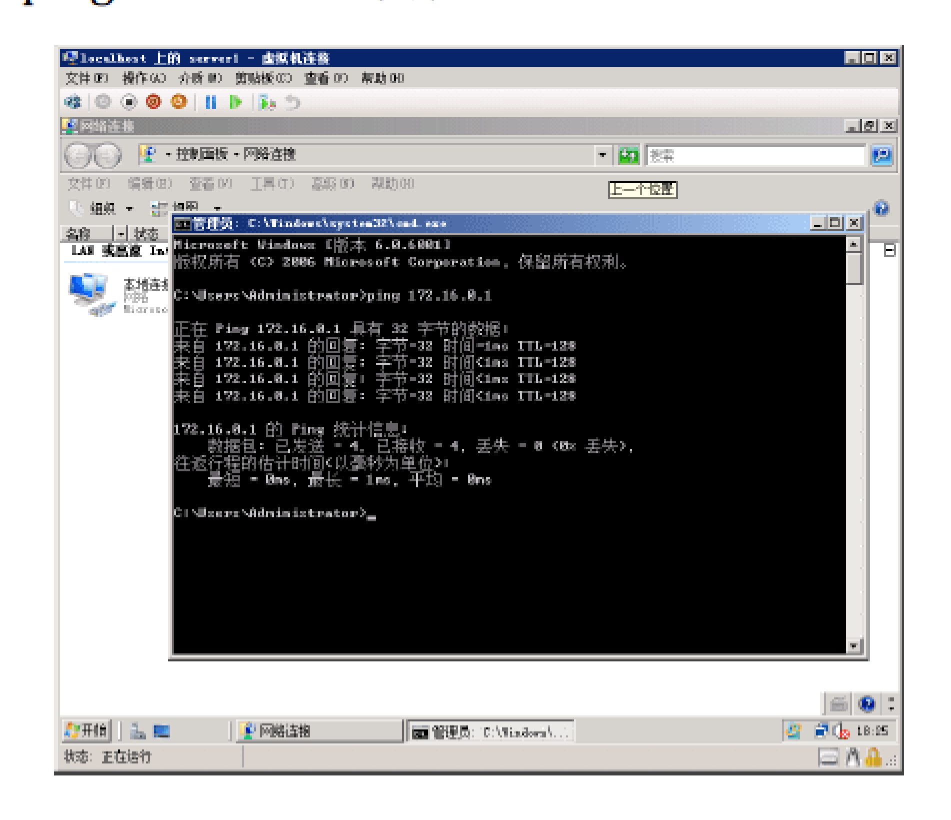


图 13-57　虚拟机和物理机能够通信

⑫　如图 13-58 所示，将 Server2 的网络适配器指定到 Office2 网络，选中“启用虚拟 LAN 标识”复选框，在下面的文本框中输入 3，单击“确定”按钮。

⑬　如图 13-59 所示，设置 Server2 的 IP 地址为 172.16.1.2，子网掩码 255.255.255.0，网关 172.16.1.1。

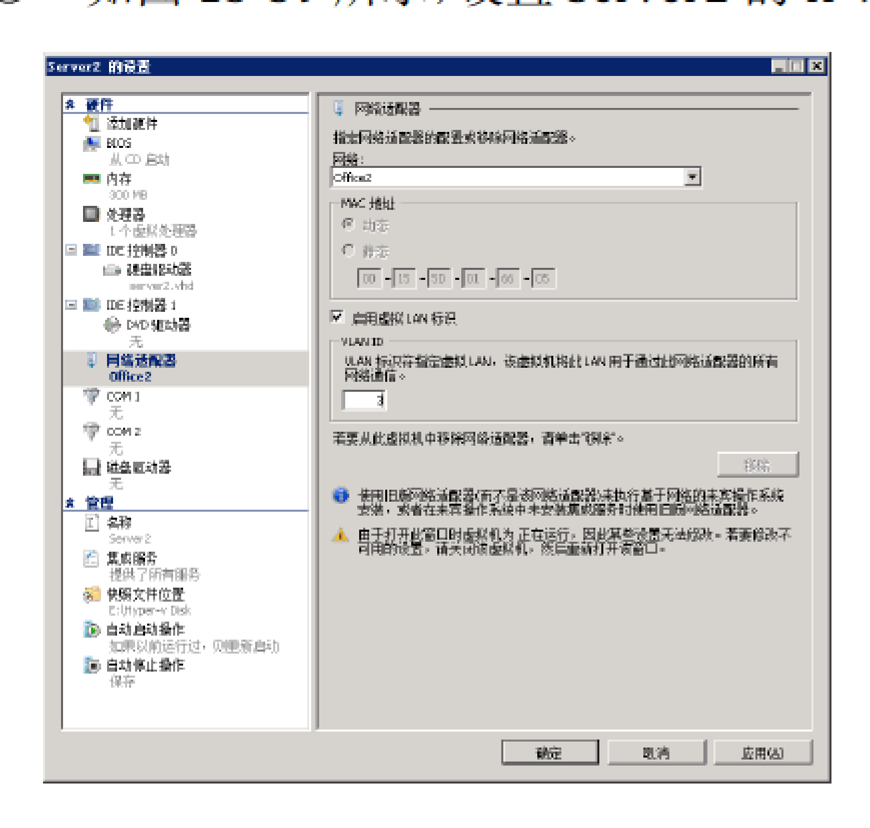


图 13-58　将 Server2 指定到网络

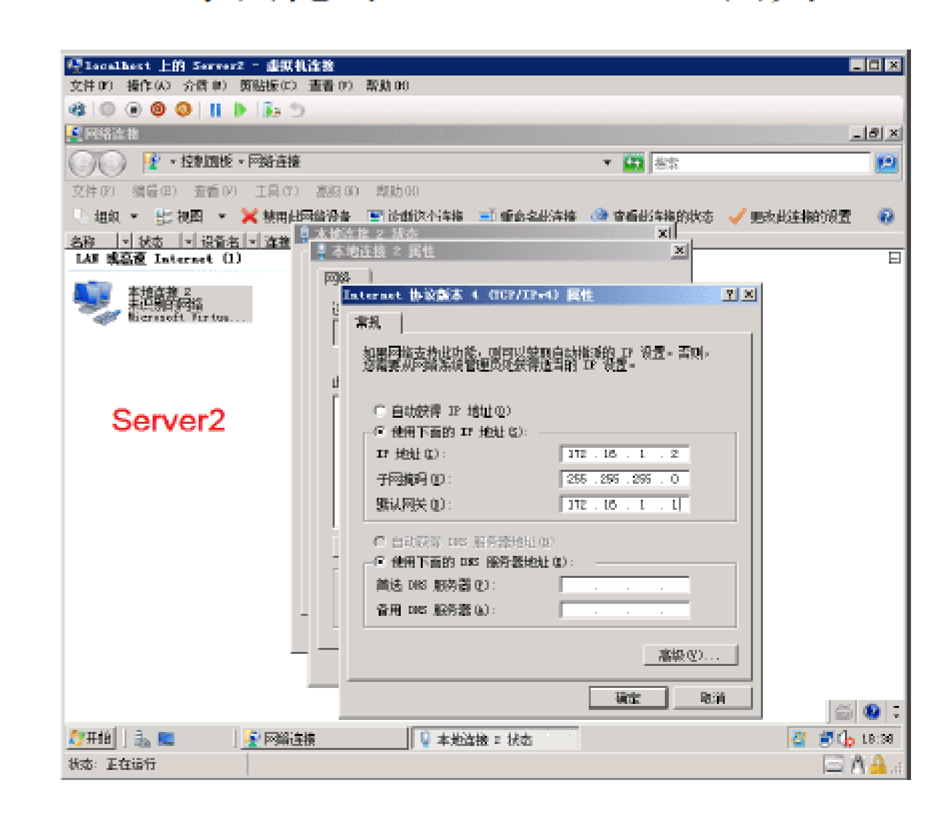


图 13-59　配置 Server2 的 IP 地址

⑭　如图 13-60 所示，在 Server2 上测试到物理机 Office2 的连接，ping 172.16.1.1 发现是通的。

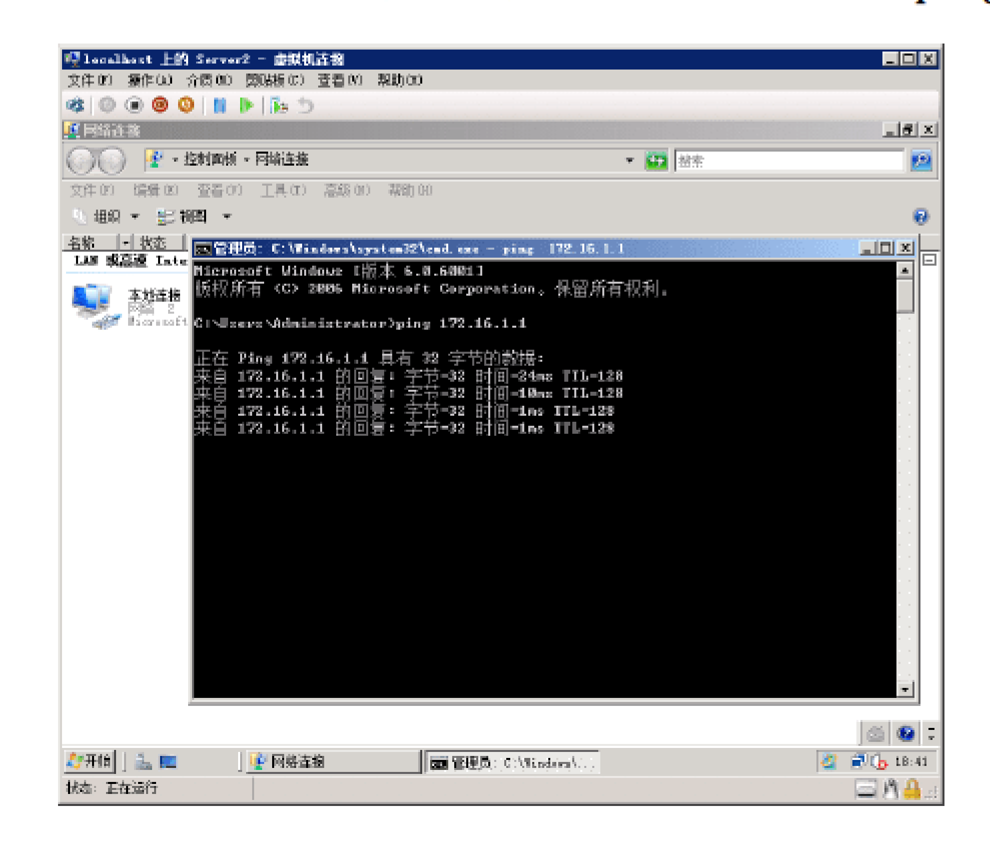


图 13-60　测试 Server2 到物理机通信

13.4.2　示例 2：创建和使用专用网络

1. 实验目标

通过创建专用网络实现虚拟机 Server1 和 Server2 之间的通信。Server1 和 Server2 不需要和物理机通信，也不需要和网络中的其他计算机通信。

将这两个虚拟机放到 VLAN 4 中，如图 13-61 所示。

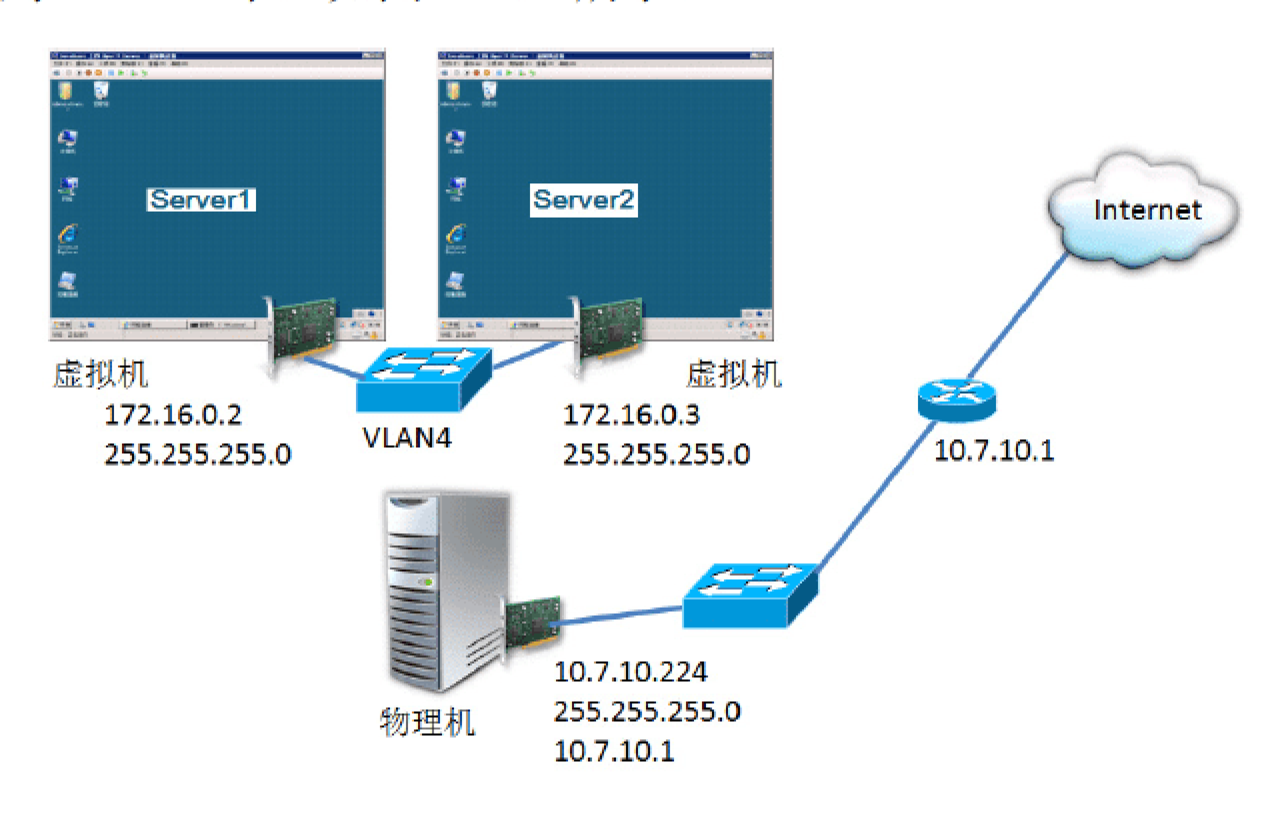


图 13-61　专用网络示意图

2. 实验步骤

① 如图 13-62 所示，打开 Hyper-V 管理工具，单击“虚拟网络管理器”按钮。

② 如图 13-63 所示，在打开的“虚拟网络管理器”对话框中，选择“新建虚拟网络”，网络类型选择“专用”，单击“添加”按钮。

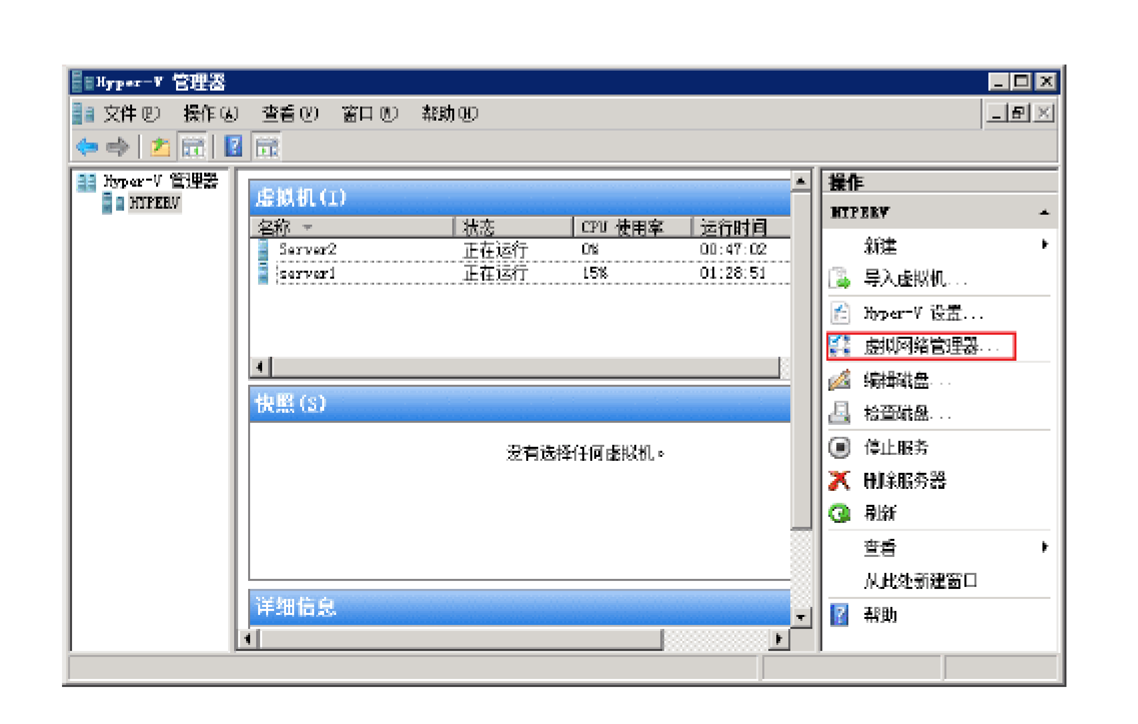


图 13-62　创建虚拟网络

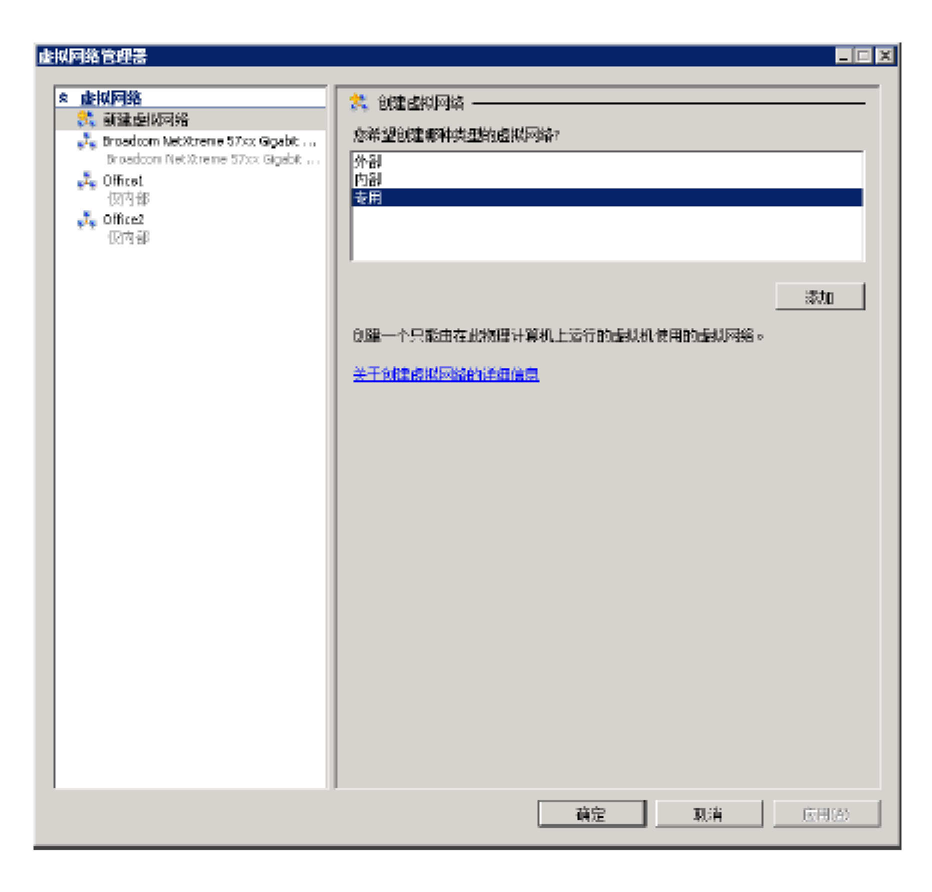


图 13-63　选择专用网络

③ 如图 13-64 所示，输入虚拟网络名称 PrivateNet，选中“专用虚拟机网络”单选按钮，单击“应用”按钮。

④ 如图 13-65 所示，更改 Server1 的设置，将网络适配器指定到 PrivateNet 网络，选中“启用虚拟 LAN 标识”复选框，输入 VLAN 编号 4，单击“确定”按钮。

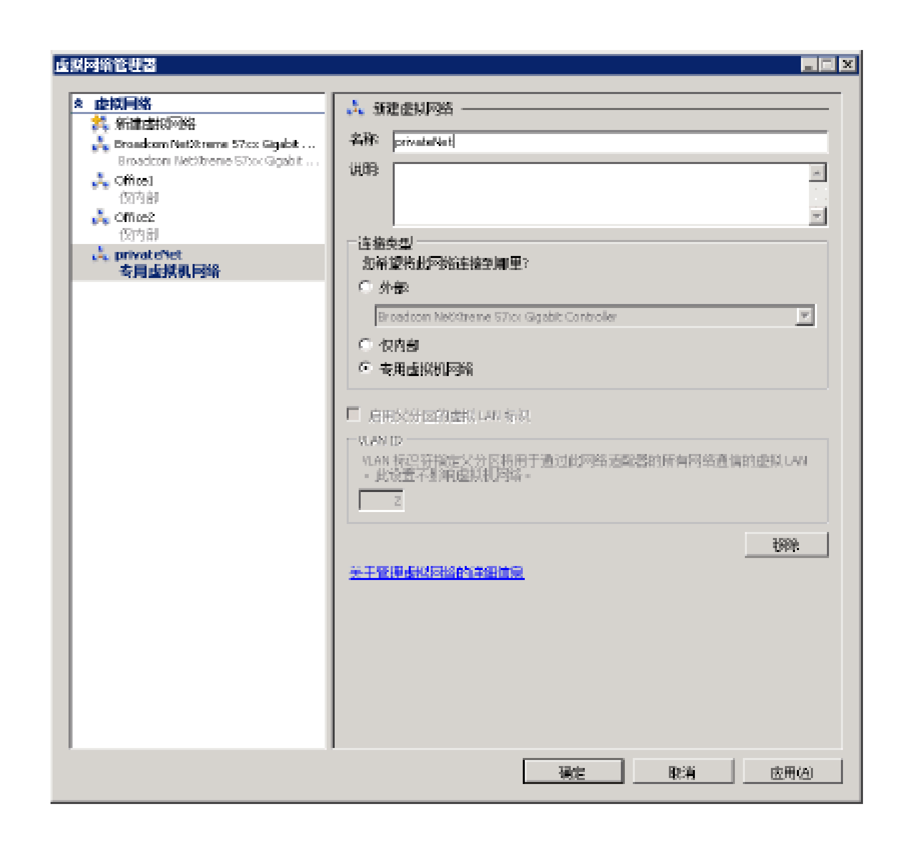


图 13-64　创建专用网络

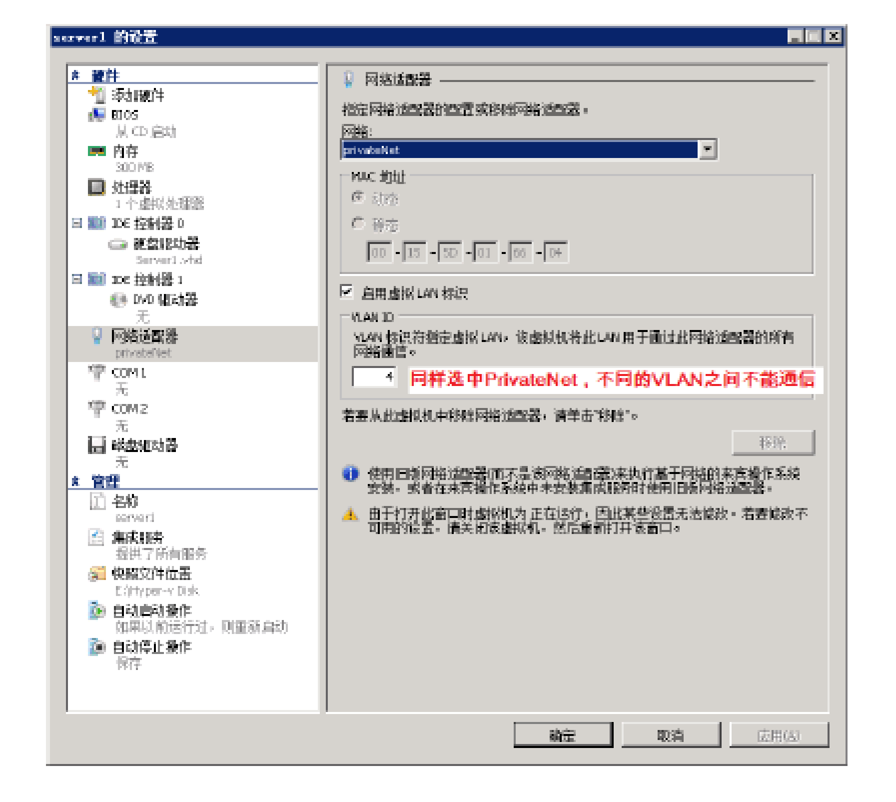


图 13-65　更改 Server1 网络

⑤　如图 13-66 所示，更改 Server2 的设置，将网络适配器指定到 PrivateNet 网络，选中“启用虚拟 VLAN 标识”，输入 VLAN 编号 4，单击“确定”按钮。

⑥　如图 13-67 所示，在 Server2 上打开网络和共享中心，启用“文件共享”。这样允许 Server1 ping 通 Server2。

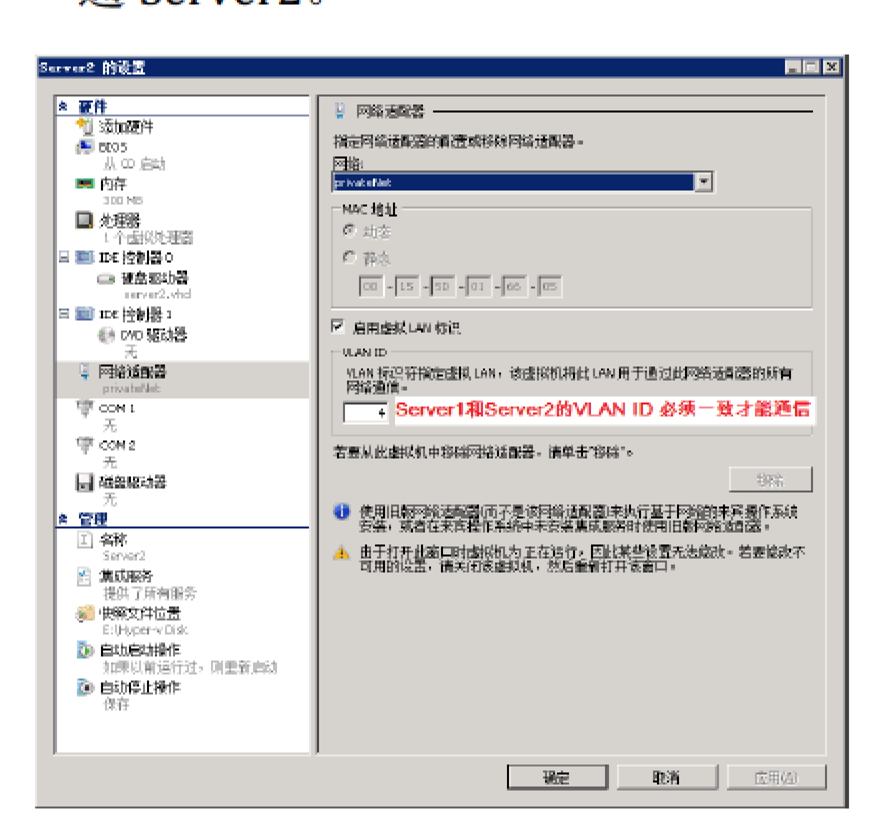


图 13-66　更改 Server2 网络



图 13-67　测试网络

⑦　如图 13-68 所示，在 Server1 上 Ping 172.16.0.3，发现网络畅通。

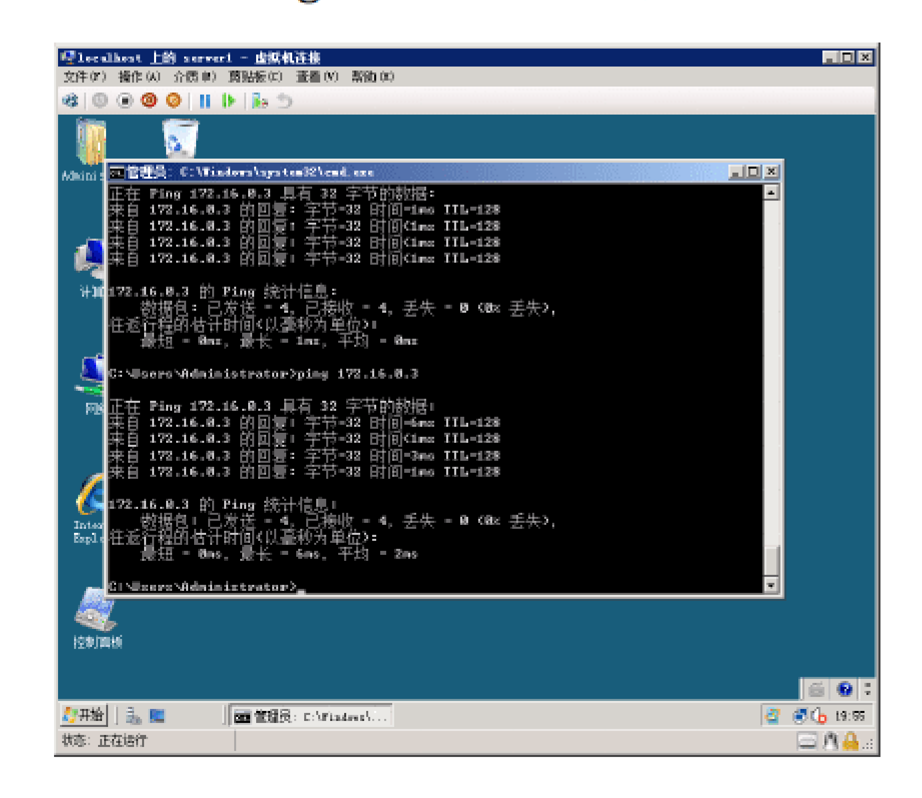


图 13-68　使用专用网络通信

13.4.3 示例 3：创建和使用外部网络

1. 实验目标

将虚拟机的网络和网络中交换机连接。

允许交换机连接到 Internet，如图 13-69 所示。

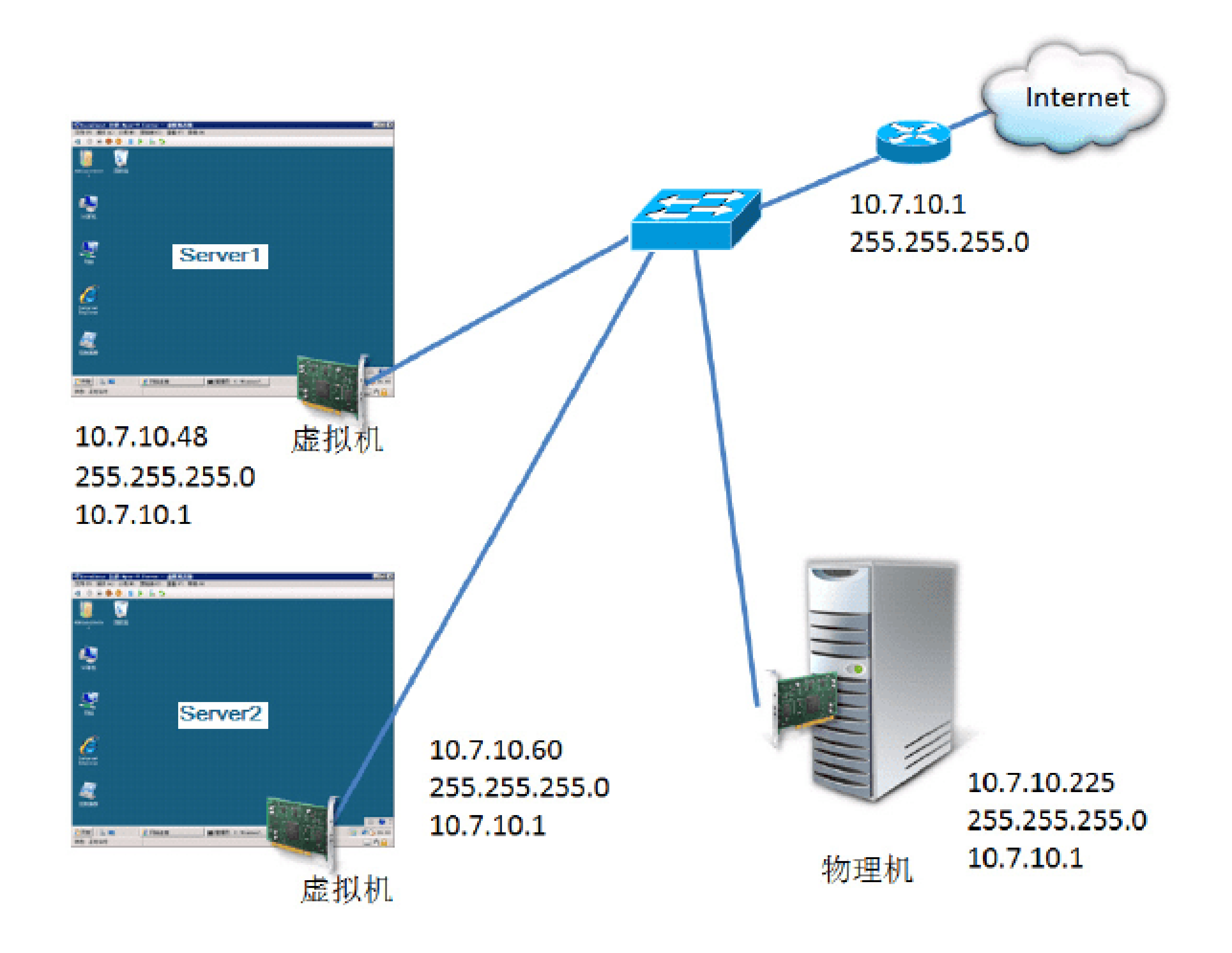


图 13-69 外部网络示意图

2. 实验步骤

① 如图 13-70 所示，更改 Server1 的设置，将网络适配指定到“Broadcom NetXtreme 57xx Gigabit Controller-虚拟网络”。

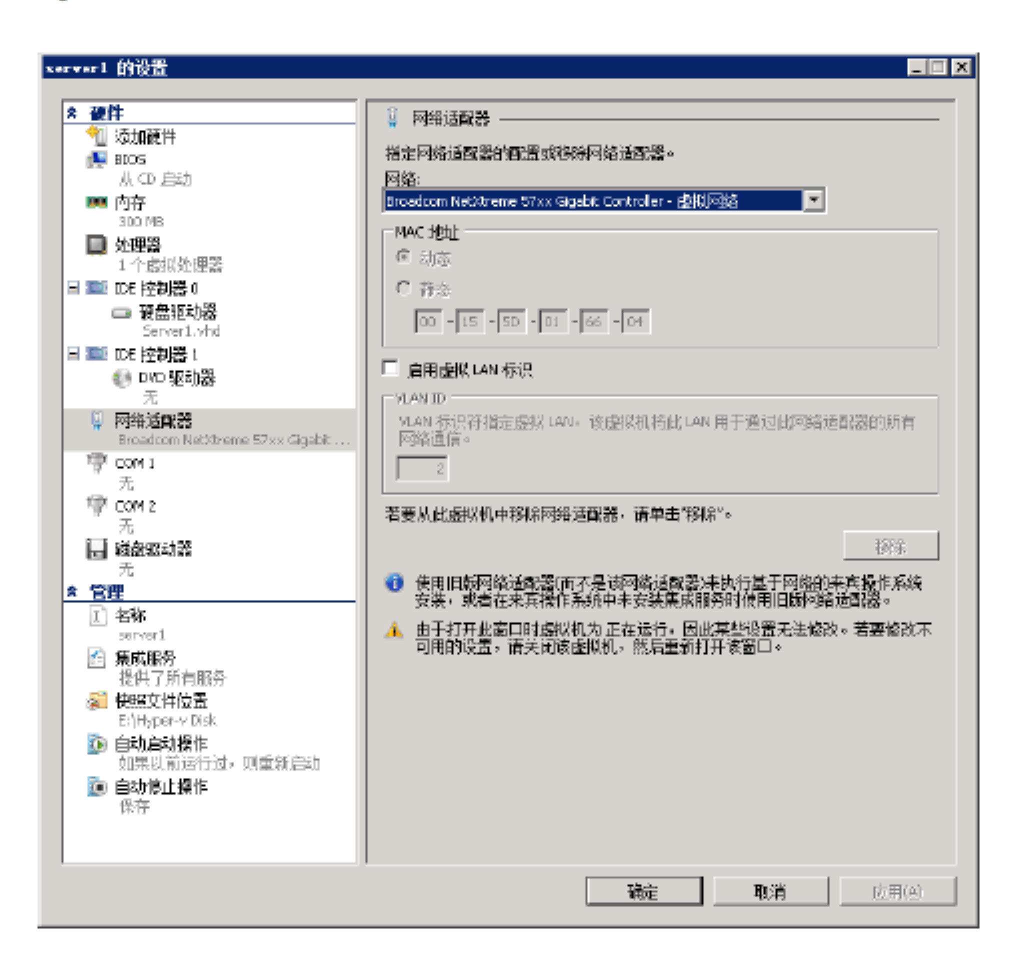


图 13-70 将网络指定到物理网络

② 更改 Server2 的设置，将网络适配指定到“Broadcom NetXtreme 57xx Gigabit Controller-虚拟网络”。

13.4.4 示例 4：将虚拟机指定到不同 VLAN

1. 实验目标

如图 13-71 所示，如果在物理机上装有两个虚拟机，网络中有两个 VLAN，计划将虚拟机 Server1 放到 VLAN10，Server2 放到 VLAN 11，路由器负责 VLAN 间路由和 Internet 连接。

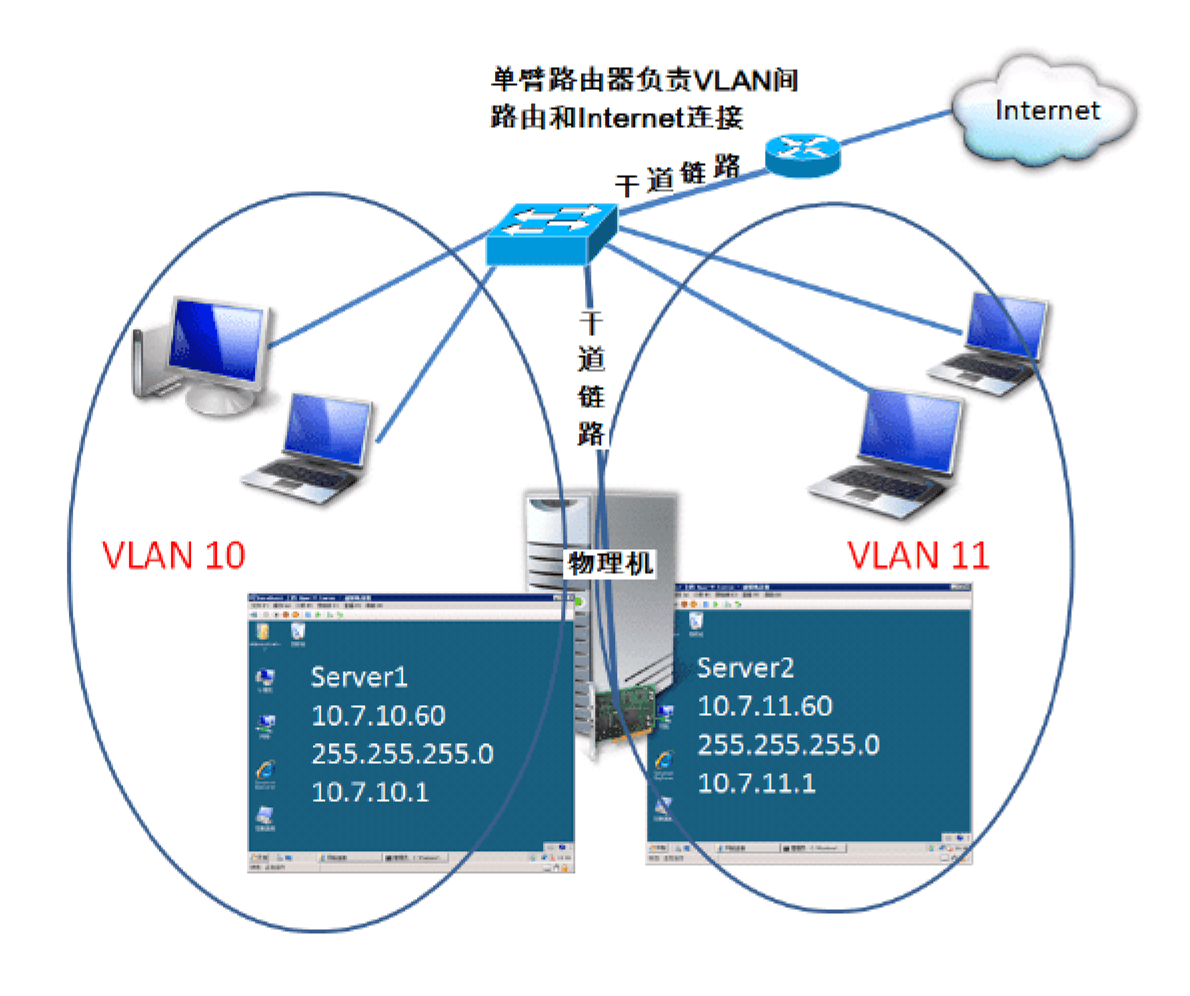


图 13-71 将虚拟机指定到不同的 VLAN

2. 实验步骤

① 将连接物理机的交换机端口设置成干道链路，连接路由器的交换机端口配置成干道链路。

② 在路由器上连接交换机干道链路的接口，配置子接口，作为 VLAN 10 和 VLAN 11 的网关。

③ 如图 13-72 所示，更改 Server1 的设置，将网络适配指定到“Broadcom NetXtreme 57xx Gigabit Controller-虚拟网络”，选中“启用虚拟 VLAN 标识”复选框，输入 VLAN ID 为 10，单击“确定”按钮。

④ 将 Server1 的 IP 地址、子网掩码和网关设置成 VLAN 10 网段的。

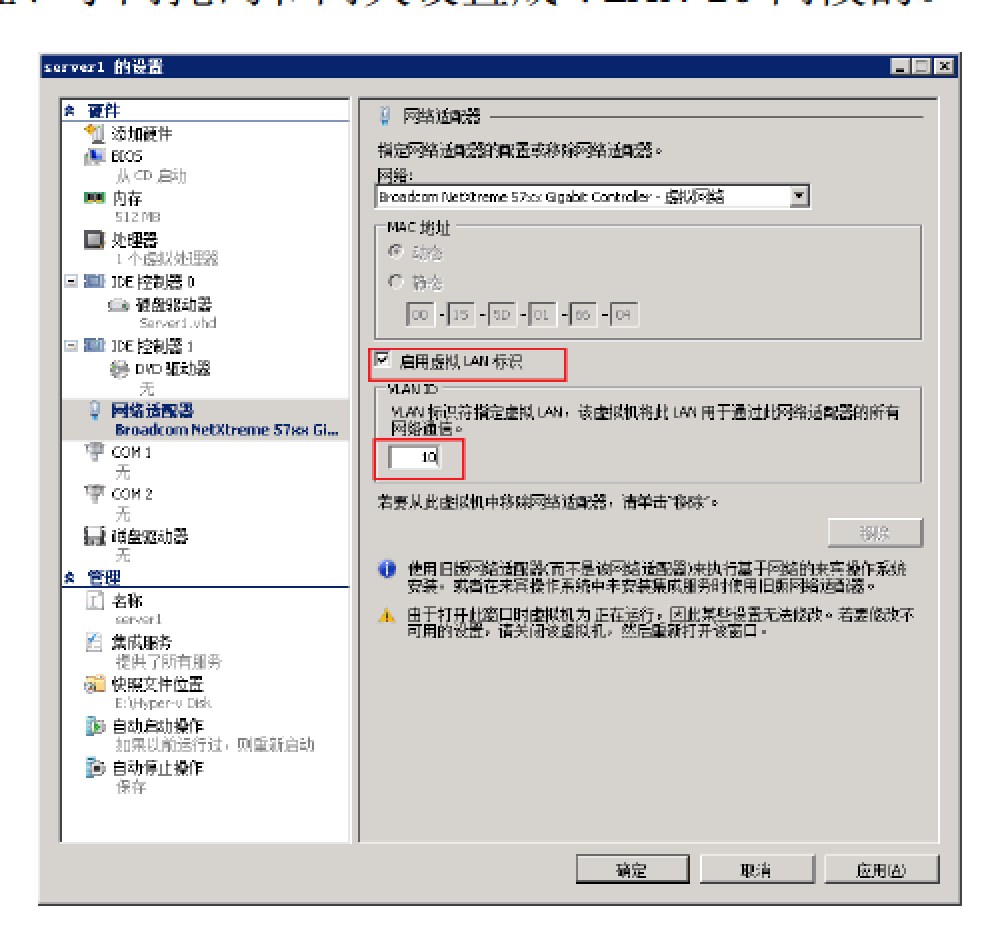


图 13-72 指定不同的 VLAN ID

⑤ 更改 Server2 的设置，将网络适配指定到“Broadcom NetXtreme 57xx Gigabit Controller-虚拟网络”，选中“启用虚拟 VLAN 标识”复选框，输入 VLAN ID 为 11，单击“确定”按钮。

⑥ 将 Server2 的 IP 地址、子网掩码和网关设置成 VLAN 11 网段的。

13.5 方案 1：整合基础架构、应用以及分支机构服务器的工作负荷

采用虚拟技术的最大推动力是可以进行服务器整合。企业在保持并加强可靠性、可扩展性和安全性等竞争优势的同时，还面临着简化管理和降低成本方面的压力。

WSv 可完美适用于数据中心和分支机构的服务器整合，使企业能够更有效地利用硬件资源。它也能使 IT 企业提高管理生产率，而且能迅速部署新的服务器来满足日益变化的业务需求，如表 13-2 所示。

表 13-2 主要整合功能

功 能	说 明
支持各种来宾操作系统	WSv 管理程序模式所支持的来宾操作系统包括 Windows Server 2008(包括服务器核心)、Linux 以及 Xen-enabled Linux。这些操作系统能利用虚拟化感知硬件和相关的性能增强功能。 WSv 中的 VM 除了能支持以上 WSv 管理程序模式中的操作系统外，还能在超过 1000 种操作系统中运行，其中包括各个版本的 DOS、Windows 以及 Windows Server(最少需要 8 个处理器的数据中心除外)。如欲获取与之兼容的操作系统列表，请登录：http://vpc.visualwin.com/
硬件虚拟化与旧式硬件仿真	使用支持来宾操作系统(如：Windows Server 2008、Linux 和 Xen-enabled Linux)的 VM 能与不存在现实对等端(如“Windows 显示适配器”)的假想设备交互作用。旧式操作系统能与作为特定设备(如 S3 Trio64 SVGA 适配器)的仿真硬件交互工作。 硬件仿真模式中的所有 VM 均使用相同的虚拟设备： 一个单核虚拟处理器(其 ID 基于实际处理器之上) 高达 3.6 GB 的系统内存 440 BX 芯片集 Adaptec 2940 PCI SCSI 控制器(多达 4 条总线) S3 Trio64 SVGA(带 2D 硬件加速功能) Intel 21140 以太网适配器(多达 4 个虚拟 NIC) 无须与设备相关联的本地虚拟网络连接 VM 也能配置为无虚拟网络连接 IDE/ATAPI 控制器 传统设备——键盘、鼠标、COM 和 LPT 端口、CMOS、PIC、DMA 等
P2V—物理到虚拟的转化	使物理服务器转换为 VM
动态硬件添加	被识别为需要更多资源的 VM 能在不停机的情况下被赋予更多的核心、内存、存储与网络

续表

功　能	说　明
CPU 资源分配	CPU 资源分配支持精细粒度控制的加权与约束方法。 高度可扩展的多线程。 每个 VM 能使用高达 100% 的单个主机处理器核心。 多个 VM 能同时执行并使用多个主机处理器核心。 可将多个 VM 托管在任意服务器，这取决于： VM 在主机上的组合处理器、内存和 I/O 负荷。 主机系统上可用的处理器、内存和 I/O 容量。 为平衡负荷管理，WSv 支持基于加权和基于约束的 CPU 资源分配。 VM 上分配的相对资源加权会与所有其他 VM 的资源相比较。相对加权较高的 VM 会从其他加权相对较低的 VM 上动态分配更多的资源。在默认设置中，所有 VM 的相对加权都是 100，这样它们的资源需求是相等的，没有一个被赋予首选项。 容量与加权算法能同时运行。 系统容量最大时也能产生连接。 相对加权能在连接期间确定资源分配
内存资源分配	WSv 能在每个 VM (per-virtual machine) 上实现灵活的内存配置，其中包括在运行的 VM 上热添加内存。 页面共享能使基于相同操作系统的 VM 在内存中共享相同的代码页面。这并不是说每个 VM 都和设备一样加载各自的静态元素并分配相关量的内存，而是说 VM 能访问相同的元素副本。如果 VM 试图改变共享页面，它就能立即被路由至唯一的页面副本。 包含对 NUMA 感知调度和内存分配的支持，可减少多个处理器插槽系统上的总线冲突。 在非 NUMA 系统上，WSv 依赖于主机操作系统的计划程序
PXE 引导	WSv 中的虚拟网卡支持预引导执行环境(PXE)的启动。该网络启动允许客户以物理服务器上的方式支持虚拟主机。 注：为充分利用该特性，PXE 基础架构需要位于主机网络上
活动目录集成	通过在网络上提供集中化的用户与计算机层级信息知识库，Active Directory 允许使用和物理机器一样的目录管理功能。Active Directory 融合了 Windows Server 2008 中管理和性能的重大改进，能从由 WSv 托管的 VM 中得到支持。 与 Active Directory 集成能实现委托管理和身份验证的来宾访问。每虚拟机 ACL (per-virtual machine ACL) 能在 Active Directory 的群组策略控制台上控制。通过它，WSv 能启用精细粒度管理控制，可将事件日志与 Active Directory 和 Microsoft 管理控制台相集成

13.6　方案 2：软件测试与开发环境的自动化和整合

WSv 使企业能够整合他们的测试和开发服务器，并自动配置 VM。

各个领域的客户都在寻求能降低成本、加速应用与基础架构安装和升级，并能全面保证质量的方法。为了能在生产前达到测试目标，必须克服多重困难。

- 网络操作。测试网络的错误配置会危害生产网络。
- 开发人员的工作效率。开发人员的工作效率会被浪费在耗时的管理任务中，例如配置测试环境和安装操作系统。
- 服务器的操作与资本性费用。高质量的应用测试需要复制生产计算环境，从而会增加预算和日程风险的昂贵的硬件和人力资源。

在 30 年前的大型机时代，为在同一系统上使用并行的测试和生产分区，VM 技术应运而生。WSv 能实现更广的测试覆盖面、更高的开发人员生产率以及更佳的用户体验。

此外，开发人员还能将 WSv 作为高效的工具来模拟单个物理服务器上的分布式应用。通常，在实验室环境中，分布式服务器应用的部署和测试需要大量的可用硬件资源与大量时间来配置硬件和软件系统，以便模拟所需方案。

WSv 是一种既节约时间又节约资源的强大解决方案，其能够在分布式服务器应用开发方案中优化硬件和人力资源的利用。WSv 在一个物理服务器上使用多个 VM，能使开发人员轻松部署和测试分布式服务器应用。WSv 将磁盘层级和虚拟网络等强大功能与机器整合价值结合在一起，能使开发人员高效模拟复杂的网络环境。这是一个非常节约时间和成本的开发环境，其扩建需要的硬件、空间和时间都较少，如表 13-5 所示。

表 13-5　主要的软件测试与开发功能

特　性	说　明
各种来宾操作系统支持	WSv 管理程序模式所支持的来宾操作系统包括 Windows Server 2008(包括服务器核心)、Linux 以及 Xen-enabled Linux。这些操作系统能利用虚拟化感知硬件和相关的性能增强功能。 WSv 中的 VM 除了能支持以上 WSv 管理程序模式中的操作系统外，还能在超过 1000 种操作系统中运行，其中包括各个版本的 DOS、Windows 以及 Windows Server(最少需要 8 个处理器的数据中心除外)
配置库	使用系统中心 VM 管理器的 WSv 能够在库中存储并管理 VM，需要时可对其进行调用。 VM 库采用了离线 VHD 控制机制，从而无须运行相关 VM 也能更改 VM
自助门户	系统中心 VM 管理器使开发与测试人员能在配置库中创建与毁坏 VM，而无须管理员的干涉
快照	快照使开发与测试人员能将 VM 系统配置回“上一个已知良好”状态。 某些开发与测试包含众多程序与操作系统安装、卸载和重新安装的等待时间。凭借 WSv 的快照特性，可将 VM 重置为此前的配置，将卸载程序或重新安装操作系统的可能性减至最小

13.7　方案 3：业务连续性与灾难恢复

WSv 可以是灾难恢复计划的一部分，这就需要跨硬件平台的应用可移植性及灵活性。将物理服务器整合至运行 VM 的较少物理机器上，能减少灾难中损坏或出故障的物理设备。在恢复过程中，可将 VM 托管在未受影响主机上的任意位置，从而不仅加速了恢复时间，而且还最大限度地提高了企业的灵活性，如表 13-6 所示。

表 13-6 主要的业务持续性和灾难恢复功能

特　性	说　明
主机和来宾群集的高度可用性	WSv 能对来宾操作系统和主机进行群集，从而启用各种高度可用的方案。主机的群集能显著增大服务器的可用性，而且成本很低，同时能启用群集中 WSv 主机的 VM 故障转移功能。使用 WSv 的企业能创建一个高可用性的 VM 环境，有效的管理计划和意外的停机方案，无须购买其他的软件工具。例如，如果系统需要更新，IT 管理员能有效地预测服务器重启。适当地配置 WSv 主机群集能使正在运行的 VM 在不停机的情况下迁移到群集中另一个主机上。 在意外的停机方案(如硬件故障)中，主机上运行的 VM 能自动迁移到下一个可用的 WSv 主机上。 来宾群集允许群集感知应用程序在 WSv 主机上的 VM 中群集
Live Backup	WSv 在无须停机的情况下备份运行的 VM 及其数据。如果服务器停机，其 VM 能在其他服务器上进行恢复并重启动，从而使服务中断最小化。 磁带备份的流程充分利用了 WSv 上的虚拟磁带驱动功能。例如，如果服务器采用了可将数据自动备份到磁带驱动器中的脚本，那么当该服务器转移到 VM 上时该流程也能使用
Health Monitoring	WSv 全面与 System Center Operations Manager 等监视工具集成，以便在出现大故障前能发现并对问题做出响应

13.8　方案 4：启用动态数据中心

数据中心在提高性能与充分利用商务智能的同时，还面临着优化硬件与设施使用的压力。WSv 能使数据中心对不断变化的需求与能量供应做出响应，并赋予其面向未来设计的灵活性。

核心功能(如对 64 位多处理器的支持，灵活的资源控制)使数据中心依靠 VM 就能完成资源密集型的工作负荷。

WSv 有助于实现动态数据中心的自我管理与操作灵活性。在业务流程中使用系统中心 VM 管理器，通过基础架构中的不同物理机能使数据中心充分利用新型应用程序与虚拟工作负荷的动态负载平衡，促进自我管理动态系统的进展。

MSC 集成

WSv 集成了 Microsoft 系统中心(MSC)。后者是新一代的动态管理工具，用于支持动态系统管理计划(DSI)。MSC 为 IT 行业的专业人士提供了工具与信息，有助于管理 IT 基础架构，在管理工具中嵌入操作知识，使系统能自我管理与修复。

Microsoft 的 DSI 策略的核心是开发并交付技术，使企业与个人生产效率更高，更能适应动态的企业需求。动态系统技术策略有三个结构元素。

- 通过使用系统模型，将操作设计嵌入 IT 基础架构之中，使之能捕捉不同知识背景人士的信息(如企业架构规划师、应用程序研发人员、IT 专业人士与工业伙伴等)。
- 知识驱动型管理能使系统捕捉模型中预期的配置与健康状态，以内部知识为系统提供一定级别的自我管理。

- 虚拟化的基础架构能将系统资源整合到一个虚拟服务池中，实现更大的灵活性并充分利用现有基础架构。虚拟化的基础架构使系统更易于按企业优先级与需求，来迅速添加、削减、移动或改变工作分配的资源。

这三个元素是构建动态系统的基础。虚拟化的基础架构能使其中的资源自由流动，知识驱动型管理机制则使这些资源满足动态企业需求，而操作设计则保证系统运行良好，如表 13-7 所示。

表 13-7　主要的动态数据中心功能

特　性	说　明
广泛的来宾操作系统支持	WSv 管理程序模式支持的来宾操作系统包括 Windows Server 2008(包括服务器核心)、Linux 和 Xen-enabled Linux。这些操作系统能充分利用虚拟化感知的硬件和相关的性能增强技术的优点。WSv 中的 VM 除了能支持以上 WSv 管理程序模式中的操作系统，还能在超过 1000 个操作系统中运行，包括各个版本的 DOS、Windows 和 Windows Server(除了最少需要 8 个处理器的 Datacenter)。如欲了解兼容的操作系统列表，请访问 http://vpc.visualwin.com/
组策略集成	组策略是一个强大的管理工具，它能一次在多个计算机和 VM 上配置特定的功能。WSv 融合了组策略，支持 VM 和虚拟服务器；并且使用了相同的工具和模板，以便在物理机上设定和执行这些策略
计数器的应用	WSv 使用计数器能使数据中心得到虚拟服务器的使用信息，加快容量规划决策

13.9　超越服务器的虚拟化

WSv 是一整套虚拟化解决方案的一部分，后者包括从桌面到数据中心的每个步骤。

Microsoft Virtual PC 2007 的桌面虚拟化能使用户运行来宾操作系统。在需求不同的操作系统的研发中，它通常用于测试垂直应用程序。除此之外，教师还可以将 Virtual PC 文件发送给课堂上所有的学生，以保证他们都在相同的设置下工作。

Microsoft SoftGrid 应用程序虚拟化技术隔离了同一操作系统上运行的各个应用程序，有助于消除潜在的冲突，使反应更迅速。应用程序会经常更新注册表(如更新虚拟注册表)，这样系统就能在不影响其他应用程序的情况下满足该应用程序的要求。应用程序的安装和卸载也快于一般的安装和卸载流程，用户自定义选项也无须手动配置。

通过 Microsoft Terminal Services 实现的显示虚拟化使远程用户可以访问寄宿于远程端的应用和操作系统。通常的应用情景是在家中或旅行时访问办公室的桌面电脑或基于服务器的应用程序。这需要给予远程用户权限，使之可以控制本地文件，登录应用程序，并连接至所需访问的桌面电脑硬件，使用其他远程方式不能访问的资源。显示虚拟化使依赖资源的应用程序可通过低功耗的笔记本或其他兼容的电脑进行访问和使用，甚至还可以允许用户运行不同的操作系统。

13.10　总　　结

WSv 是一项面向 Windows Server 2008 平台的低成本、全面支持的服务器虚拟技术。Microsoft 在基于管理程序和硬件辅助虚拟化方面的进步，极大地改进了 VM 的可靠性和可升级性。它使最耗资源的工作

负荷也能在动态 VM 上运行。WSv 的工业标准管理工具能使系统管理员在熟悉并得到广泛支持的界面上，管理虚拟服务器和物理服务器。

WSv 允许企业整合结构、应用程序和分支办公室服务器工作负荷。WSv 能理想地用于数据中心和分支办公室服务器的整合，使企业能更有效地利用硬件资源。它也能使 IT 提高管理生产力，迅速部署新的服务器来满足不断变化的商务需求。WSv 能使商务活动对其测试和研发的服务器群进行整合，自动提供 VM。WSv 也是恢复计划的一部分，而后者需要硬件平台上应用程序的可迁移性和灵活性。同时，WSv 使数据中心面对变化的需求，能迅速地做出反应，并让其拥有超前设计的性能和灵活性。

第 14 章　高可用群集和 QoS

随着互联网的迅速发展，应用服务器工作量的日益增加，负载平衡技术的应用越加广泛。而在众多的负载平衡技术中，网络负载平衡技术由于其优势，已成为目前使用最为广泛的技术。

QoS 的英文全称为 Quality of Service，中文名为“服务质量”。QoS 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

关键词

- 网络负载平衡的使用场景
- 配置 Windows Server 2008 网络负载平衡
- QoS

14.1 Windows Server 2008 实现网络负载平衡

Windows Server 2008 中的网络负载平衡 (NLB) 功能可以增强 Internet 服务器应用程序 (如在 Web、FTP、防火墙、代理、虚拟专用网络 (VPN) 以及其他执行关键任务的服务器上使用的应用程序) 的可用性和可伸缩性。运行 Windows Server 2008 的单个计算机只能提供有限的服务器可靠性和可伸缩性能。但是，通过将运行 Windows Server 2008 的其中一个产品的两台或多台计算机的资源组合到单个虚拟群集中，NLB 便可以提供 Web 服务器和其他执行关键任务服务器所需的可靠性和性能

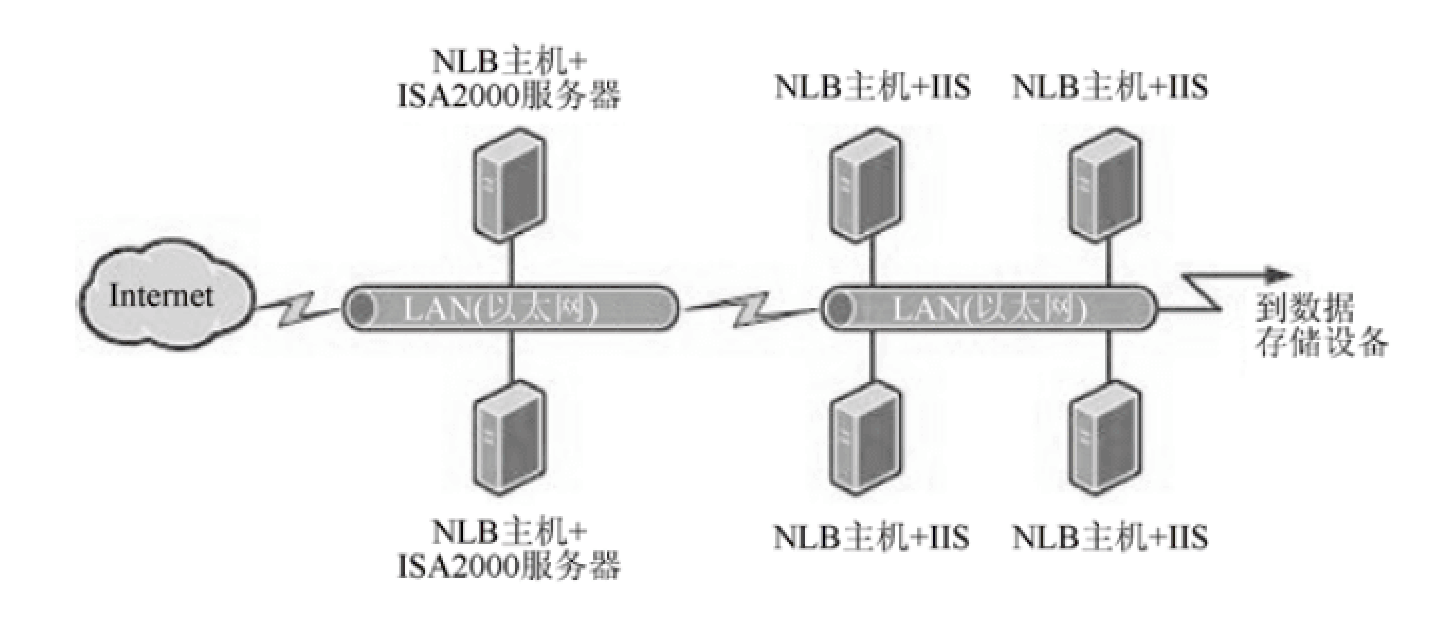


图 14-1　网络负载平衡示意图

图 14-1 描述了两个连接的网络负载平衡群集。第一个群集由两个主机组成，第二个群集由四个主机组成。这是如何使用 NLB 的一个示例。

每个主机都运行所需的服务器应用程序(如用于 Web、FTP 和 Telnet 服务器的应用程序)的单个副本。NLB 在群集的多个主机中分发传入的客户端请求。可以根据需要配置每个主机处理的负载权重，还可以向群集中动态地添加主机，以处理增加的负载。此外，NLB 还可以将所有流量引导至指定的单个主机，该主机称为默认主机。

NLB 允许使用相同的群集 IP 地址集指定群集中所有计算机的地址，并且它还为每个主机保留一组唯一专用的 IP 地址。对于负载平衡的应用程序，当主机出现故障或者脱机时，会自动在仍然运行的计算机之间重新分发负载。当计算机意外出现故障或者脱机时，将断开与出现故障或脱机的服务器之间的活动连接。但是，如果用户有意关闭主机，则可以在使计算机脱机之前，使用 drainstop 命令维护所有活动的连接。任何一种情况下，都可以在准备好时将脱机计算机明确地重新加入群集，并重新共享群集负载，以便使群集中的其他计算机处理更少的流量。

NLB 群集中的主机会交换检测消息以保持有关群集成员身份的数据的一致性。默认情况下，当主机在 5 s 之内未能发送检测消息时，该主机便出现了故障。当主机出现故障时，群集中的剩余主机将聚合在一起并执行以下操作。

- 确定哪些主机仍然是群集中的活动成员。
- 选择优先级最高的主机作为新的默认主机。
- 确保所有新的客户端请求都由仍然活动的主机进行处理。

在聚合期间，仍然活动的主机会查找一致的检测信号。如果无法发送检测信号的主机开始提供一致的检测信号，则它会在聚合过程中重新加入群集。当新的主机尝试加入群集时，它会发送检测消息，该消息也会触发聚合。当所有群集主机对当前的群集成员身份达成一致之后，会向剩余主机重新分发客户端负载，

并完成聚合。

通常聚合只需几秒钟，因此由群集中断的客户端服务是非常少的。在聚合期间，仍然活动的主机会继续处理客户端请求，而不会影响现有连接。如果所有主机在几个检测期间报告的群集成员身份和分发映射都一致，则聚合结束。

14.1.1　NLB 中的新增功能

对于 Windows Server 2008，NLB 包括以下改进。

- 支持 IPv6。NLB 对所有通信都完全支持 IPv6。所有 NLB 组件都支持 IPv6 地址，并且可以将这些地址配置为主要群集 IP 地址、专用 IP 地址和虚拟 IP 地址。此外，还可以作为纯 IPv6 以及在 IPv6 over IPv4 模式下对 IPv6 进行负载平衡。
- 支持 NDIS 6.0。NLB 驱动程序使用 NDIS 6.0 轻型筛选模型。NDIS 6.0 保持与早期 NDIS 版本的向后兼容性。NDIS 6.0 的设计包括增强的驱动程序性能和可伸缩性以及简化的 NDIS 驱动程序模型。
- WMI 增强。MicrosoftNLB 命名空间添加了对 IPv6 的多个专用 IP 地址的支持，包括以下地址。
  - MicrosoftNLB 命名空间中的类支持 IPv6 地址(除了 IPv4 地址之外)。
  - MicrosoftNLB_NodeSetting 类支持多个专用的 IP 地址，方法是在 DedicatedIPAddresses 和 DedicatedNetMasks 中指定这些地址。
- 改进了拒绝服务 (DoS) 攻击和计时器饥饿保护。使用回调接口，NLB 可以在攻击期间或者节点负载过高时检测并通知应用程序。当群集节点过载或者受到攻击时，ISA 服务器使用该功能。
- 支持每个节点使用多个专用 IP 地址。NLB 完全支持为每个节点定义多个专用 IP 地址，而以前只支持每个节点使用一个专用 IP 地址。当客户端由 IPv4 和 IPv6 通信组成时，ISA 服务器可以使用该功能来管理每个 NLB 节点。
- 支持滚动升级。NLB 支持从 Windows Server 2003 到 Windows Server 2008 的滚动升级。
- 通过网络负载平衡管理器综合管理。不再需要使用网络连接工具配置 NLB 群集，只需通过 Windows Server 2008 中的 NLB 管理器即可执行 NLB 群集配置。这样便可以最大限度地减少可能因群集主机之间设置不一致引起的 NLB 配置问题。

14.1.2　NLB 配置

NLB 作为 Windows 网络驱动程序运行，如图 14-2 所示，它的操作对于 TCP/IP 网络堆栈是透明的。

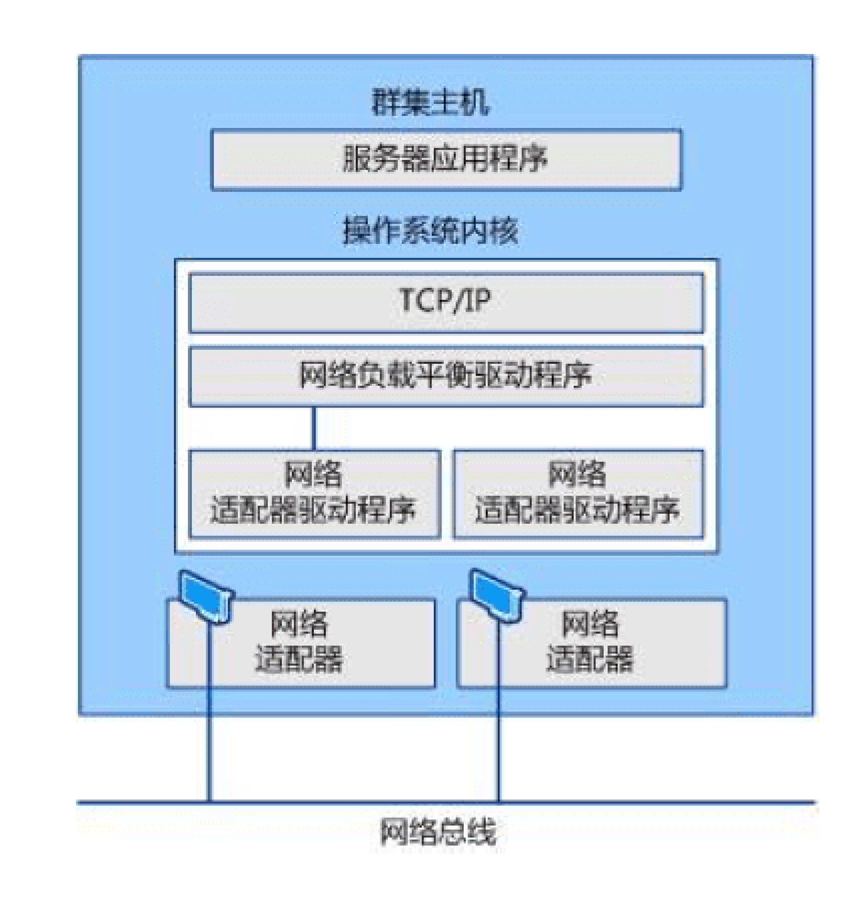


图 14-2　网络负载平衡

网络负载平衡的功能

- 可伸缩性：可伸缩性是量度计算机、服务或应用程序如何更好地改进以满足持续增长的性能需求的标准。对于 NLB 群集而言，可伸缩性是指当群集的全部负载超过其能力时逐步将一个或多个系统添加到现有群集中的功能。以下详细介绍了 NLB 的可伸缩性功能。

- 平衡 NLB 群集上对各个 TCP/IP 服务的负载请求。
- 在一个群集中最多支持 32 台计算机。
- 平衡群集中多个主机之间的多个服务器负载请求(来自同一个客户端或者来自几个客户端)。
- 支持在负载增加时，能够在不关闭群集的情况下向 NLB 群集中添加主机。
- 支持在负载降低时，能够从群集中删除主机。
- 通过全部实现管道化提高性能并降低开销。管道允许向 NLB 群集发送请求，而无须等待响应上一个发送的请求。

■ 高可用性：通过最大限度地减少停机时间，高可用系统能够可靠地提供可接受级别的服务。NLB 包括一些内置功能，可以通过自动执行以下操作来提供高可用性。

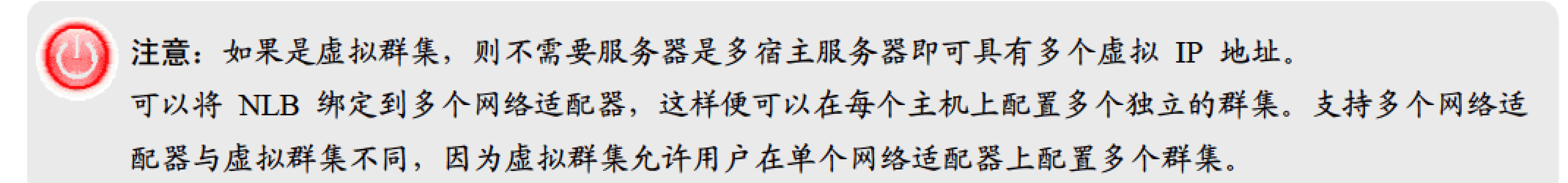
- 检测发生故障或脱机的群集主机并对其进行恢复。
- 在添加或删除主机时平衡网络负载。
- 在 10 s 之内恢复并重新分发负载。

■ 可管理性：NLB 提供以下可管理性功能。

- 使用 NLB 管理器，可以从单个计算机管理和配置多个 NLB 群集和群集主机。
- 使用端口管理规则，可以为单个 IP 端口或一组端口指定负载平衡行为。
- 可以为每个网站定义不同的端口规则。如果对多个应用程序或网站使用相同的一组负载平衡服务器，则端口规则基于目标虚拟 IP 地址(使用虚拟群集)。
- 使用可选的单主机规则，可以将所有客户端请求引导至单个主机。NLB 将客户端请求路由到运行特定应用程序的特定主机。
- 可以阻止对某些 IP 端口进行不需要的网络访问。
- 可以在群集主机上启用 Internet 组管理协议 (IGMP) 支持，以控制交换机广播(在多播模式中操作时)。
- 使用 shell 命令或脚本，可以从运行 Windows 的任何联网计算机上远程启动、停止和控制 NLB 操作。
- 可以查看 Windows 事件日志以检查 NLB 事件。NLB 在事件日志中记录所有操作和群集更改。

■ 易用性：NLB 提供了许多便于使用的功能。

- 可以作为标准的 Windows 网络驱动程序组件安装 NLB。
- NLB 不需要更改任何硬件即可启用和运行。
- 使用 NLB 管理器可以新建 NLB 群集。
- 使用 NLB 管理器，可以从一台远程或本地计算机上配置和管理多个群集以及群集的所有主机。
- NLB 允许客户端使用单个逻辑 Internet 名称和虚拟 IP 地址(称为群集 IP 地址，它保留每台计算机的各个名称)访问群集。NLB 允许多宿主服务器具有多个虚拟 IP 地址。



注意： 如果是虚拟群集，则不需要服务器是多宿主服务器即可具有多个虚拟 IP 地址。
可以将 NLB 绑定到多个网络适配器，这样便可以在每个主机上配置多个独立的群集。支持多个网络适配器与虚拟群集不同，因为虚拟群集允许用户在单个网络适配器上配置多个群集。

- 不需要修改服务器应用程序即可在 NLB 群集中运行。
- 如果群集主机出现故障并且后来又恢复联机，则可以将 NLB 配置为自动将该主机添加到群

集。之后，添加的主机将能够开始处理来自客户端的新的服务器请求。
- 可以在不打扰其他主机上群集操作的情况下使计算机脱机进行预防性的维护。

■ NLB 群集最早出现在 Windows 2000 Server 的 Advanced Server 系统中，在 Windows Server 2008 的某些版本中均提供了此项功能。

14.2 NLB 的使用场景

下面介绍使用网络负载平衡的使用场景。

14.2.1 Web 站点的负载平衡

某学院的 Web 站点为了实现负载平衡，避免单点故障，考虑使用镜像站点实现冗余和负载平衡，这几个镜像站点放在 DMZ 区，网站使用的数据库放在企业的内网中。

如图 14-3 所示，通过使用 NLB 技术，这几个 Web 服务器使用公共的地址 22.34.3.100 访问 DMZ 中的 Web 服务器。来自互联网的请求将会自动地由这几个服务器均摊。

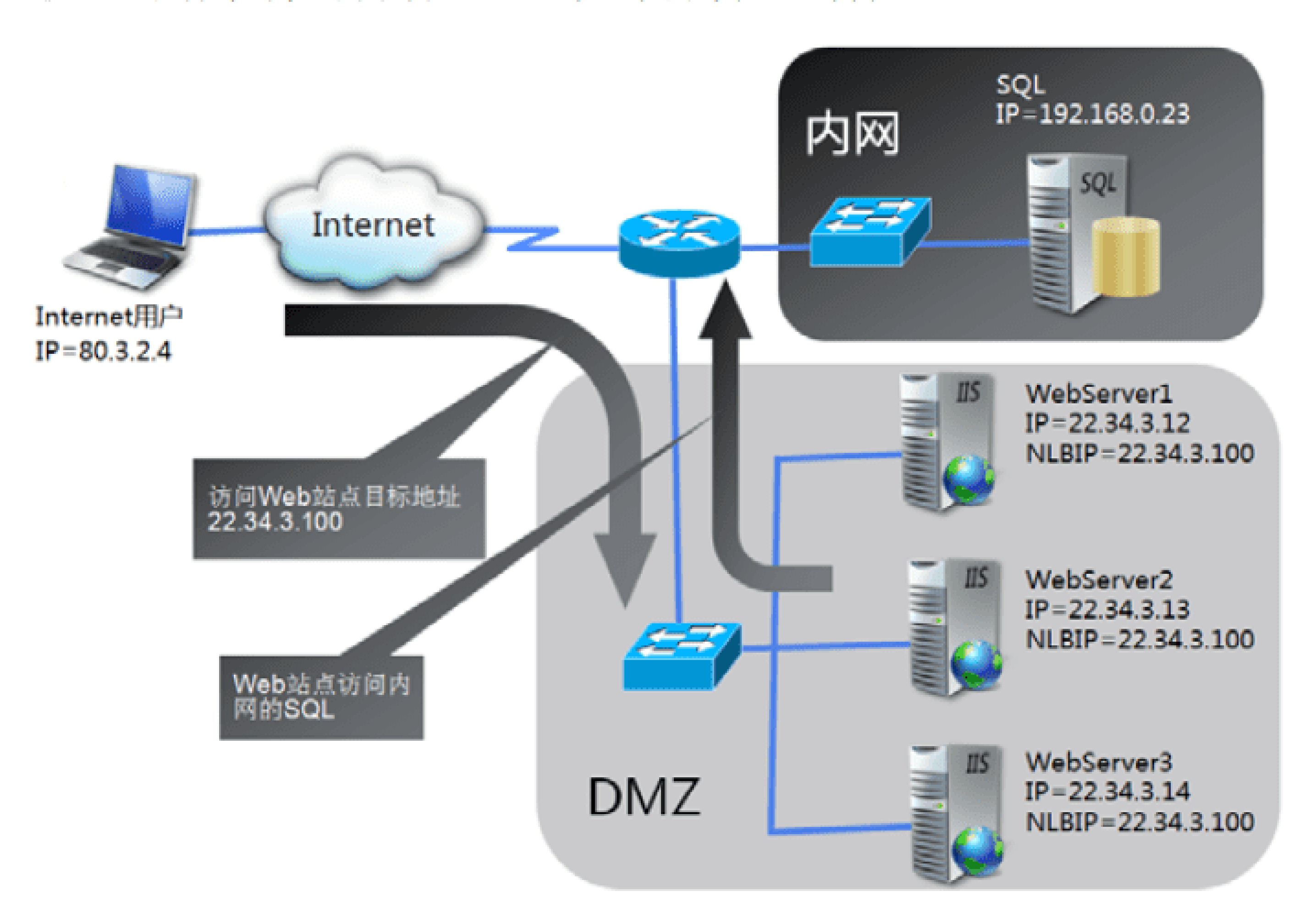


图 14-3　Web 站点网络负载平衡

14.2.2 终端服务负载平衡

某汽车生产厂正在开发应用软件，该应用软件正处于试运行期间，如果在每个财务人员的计算机上安装该软件，软件升级更新很不方便。为了方便起见，如图 14-4 所示，将测试版的软件安装在终端服务器 TS1 和 TS2 上，财务人员通过终端服务使用 TS1 和 TS2 上的软件，使用 NLB 技术，财务人员的计算机连接 NLBIP 地址，将会把来自财务人员的请求分摊到两个终端服务器。这两个服务器上的软件操作的是同一个数据库，因此用户使用任何一个终端服务器上的程序，操作的数据都是一样的。

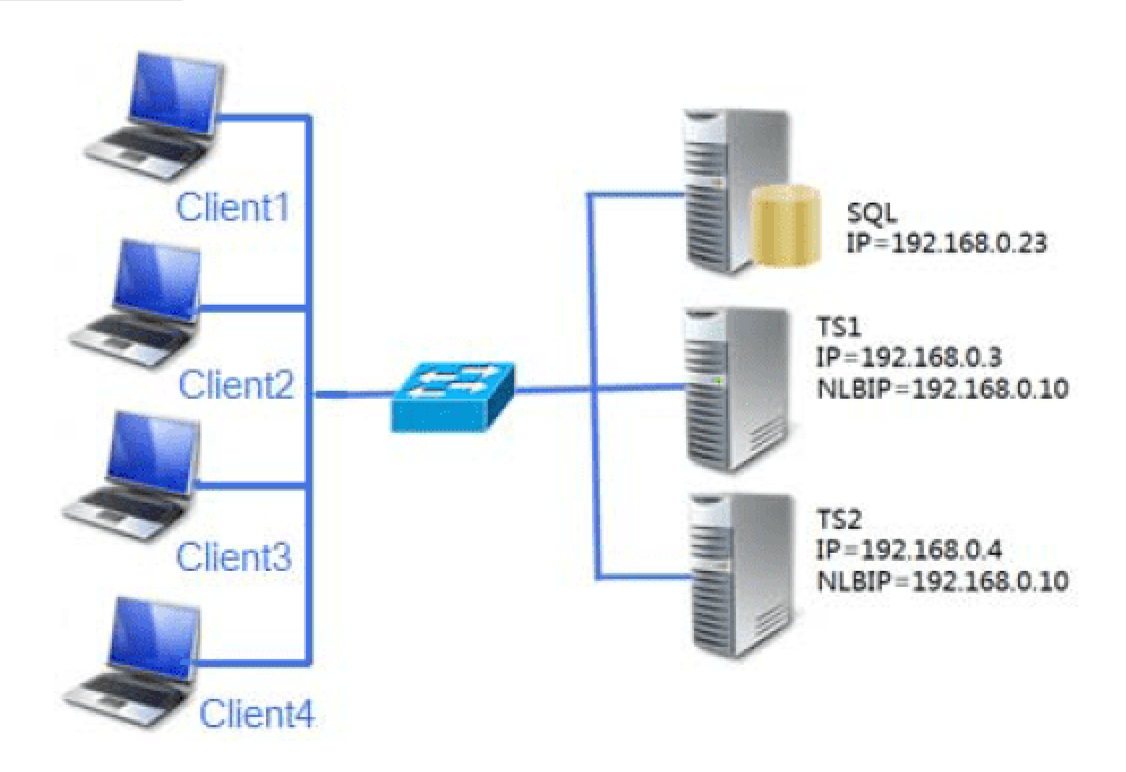


图 14-4 终端服务器负载平衡

14.2.3 网关的负载平衡

如图 14-5 所示，某单位有两个办公室 OfficeA 和 OfficeB，分别有两个 ADSL 接入 Internet。现在想实现两条线路的负载平衡和冗余。首先需要将两个办公室的交换机连接起来，再将这两个办公室的 IP 地址设置成一个网段，将公用的 IP 地址设置成 192.168.0.1，OfficeA 和 OfficeB 的计算机网关设置成 NLBIP 192.168.0.1。如果 OfficeB 中连接 ADSL 的计算机出现故障，断掉局域网的网线，两个办公室的计算机将会使用 OfficeA 中的 ADSL 上网。如果两个网线都能用，访问 Internet 的流量将会从两个 ADSL 负载平衡。

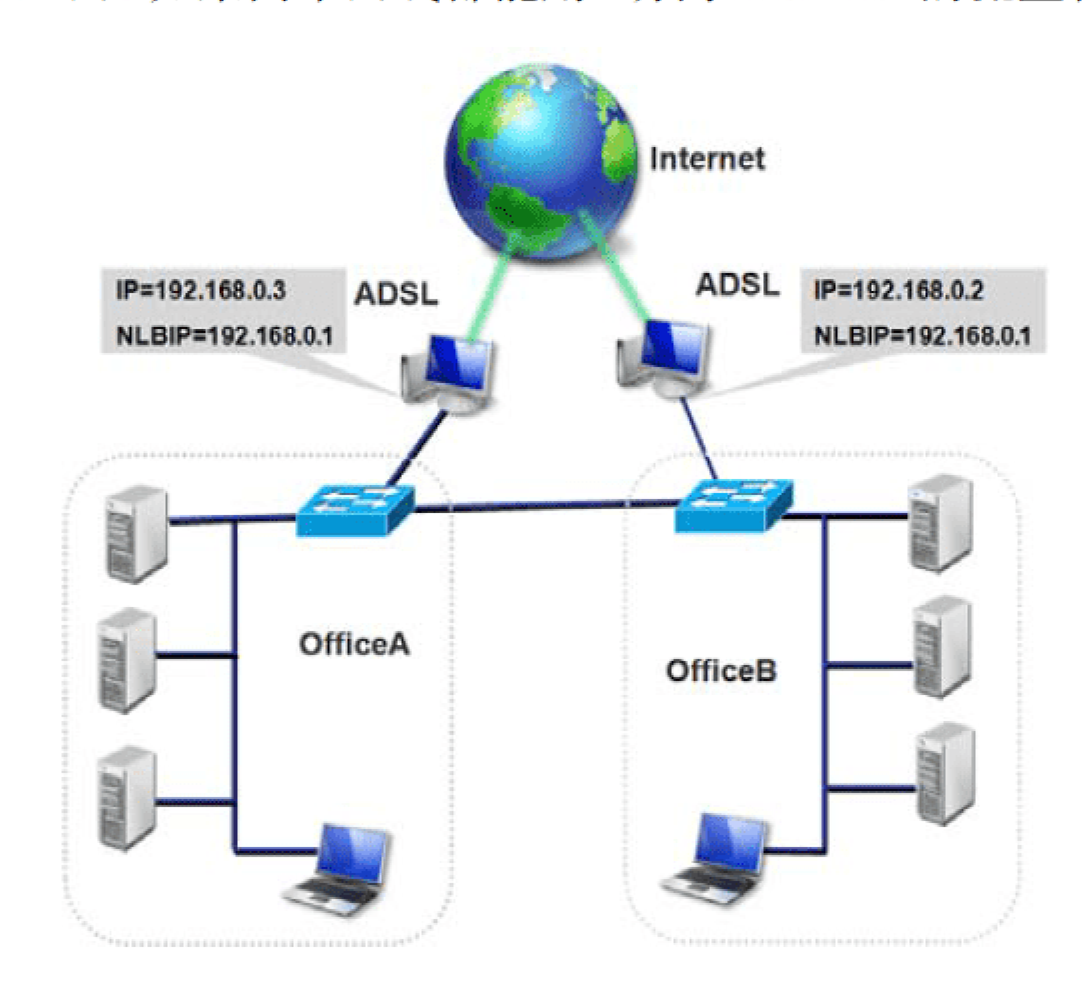


图 14-5 网关负载平衡

14.3 在 Windows Server 2008 上配置 NLB

1. 实验环境

DCServer 是 Ess.com 域的域控制器。

Fileserver 和 Research 属于 Ess.com 域，安装有 Windows Server 2008 企业版。

Sales 计算机是 Ess.com 域的成员，安装 Vista 企业版。

2. 实验要求

实现 FileServer 和 Research 服务器的网络负载平衡。



注意：如果给工作组中的计算机配置 NLB，这两个服务器的管理员账号和密码设置成一致的，这样才能在一台服务器上将另一台服务器添加过来进行管理，否则提示没权限。FileServer 和 Research 必须是静态地址，必须在一个网段，如图 14-6 所示。

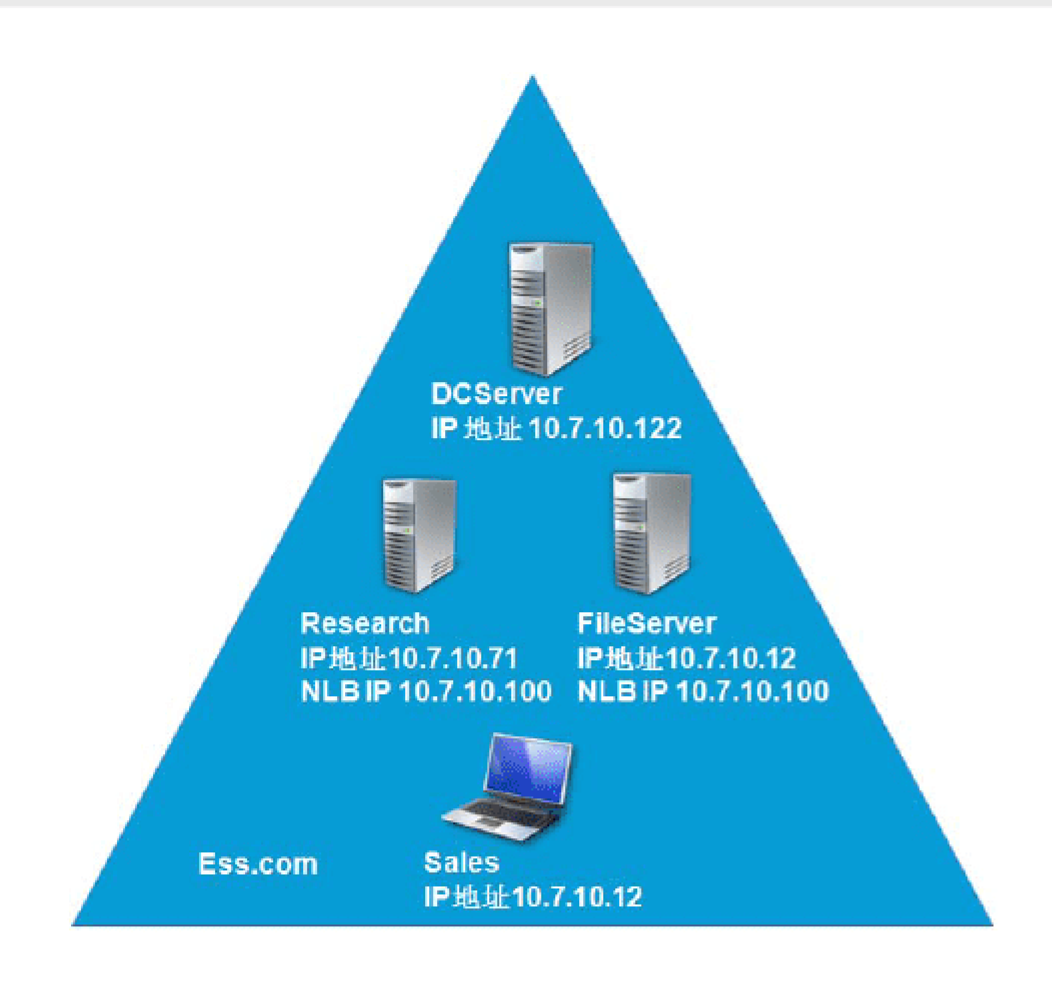


图 14-6　实验环境

14.3.1　配置 Windows Server 2008 NLB

① 以域管理员的身份登录到 Research，单击开始按钮，打开服务器管理器，如图 14-7 所示，单击“添加功能”按钮。

② 如图 14-8 所示，在弹出的“选择功能”界面中，选中“网络负载平衡”复选框。

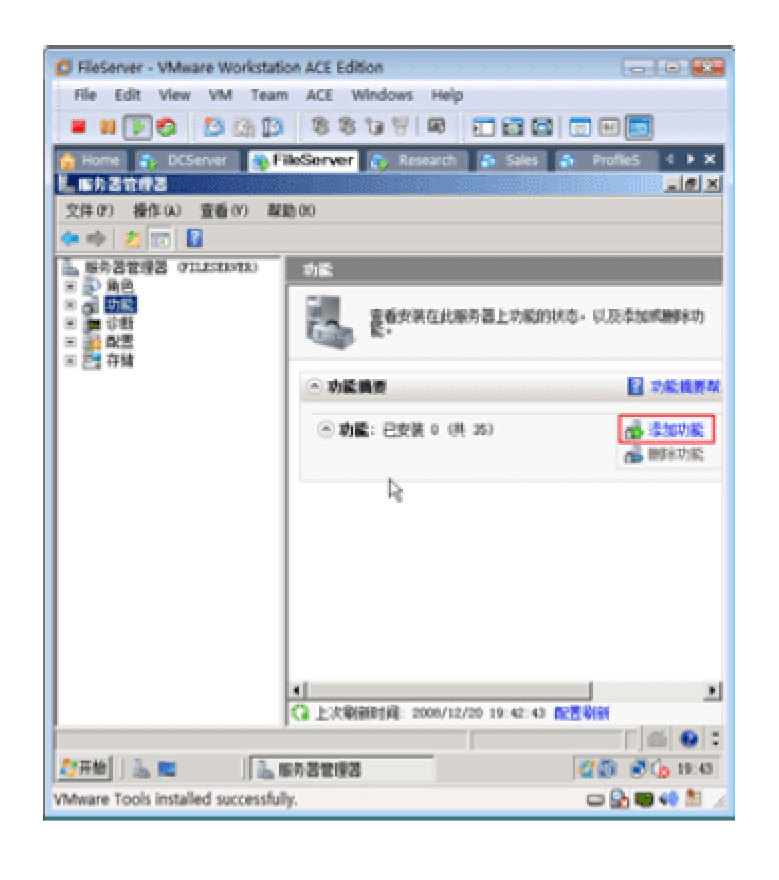




图 14-7　添加功能

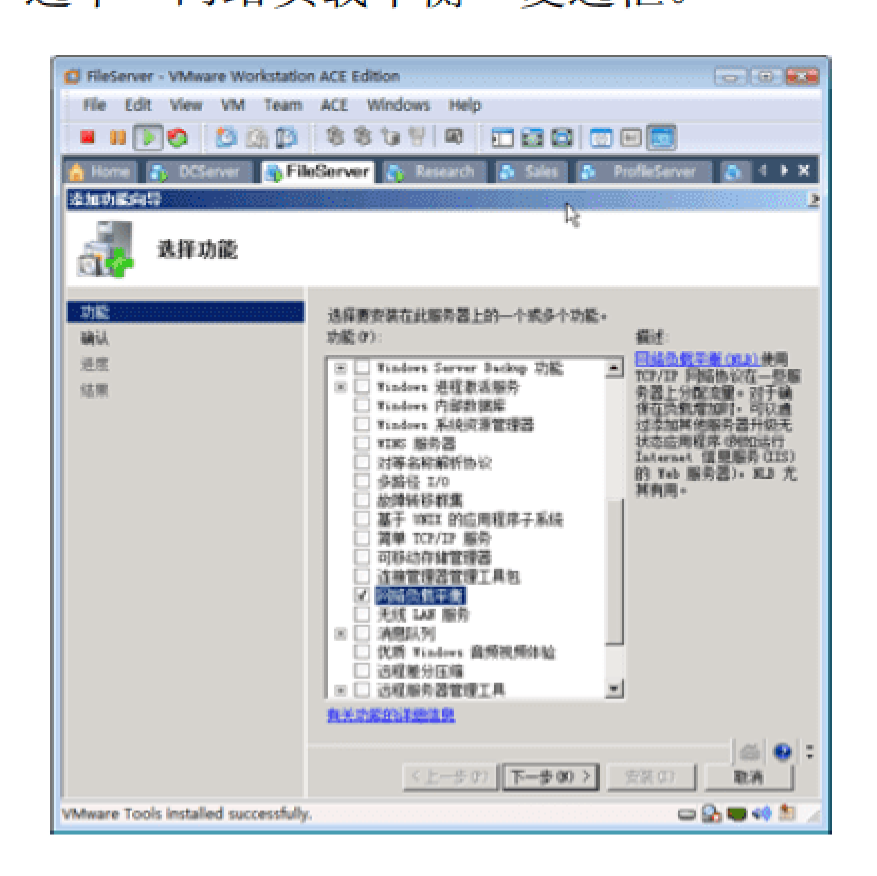


图 14-8　选择功能

③ 单击“下一步”按钮，完成安装。

④ 在另一 Research 服务器上，也安装网络负载平衡功能。

⑤ 如图 14-9 所示，在 FileServer 上，选择“开始”→“程序”→“管理工具”→“网络负载平衡管理器”命令，打开“网络负载平衡管理器”窗口，在左侧窗格中右击“网络负载平衡群集”，从弹出的快捷菜单中选择“新建群集”命令。

⑥ 如图 14-10 所示，输入 fileserver，单击“连接”按钮，再单击“下一步”按钮。

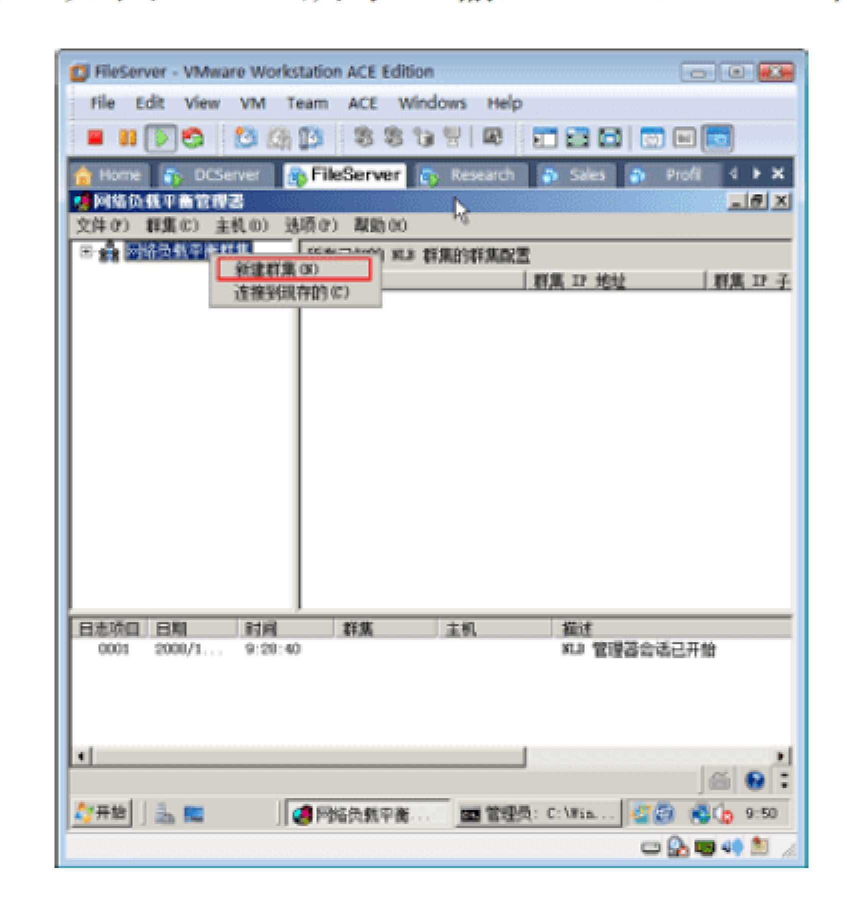




图 14-9　新建群集

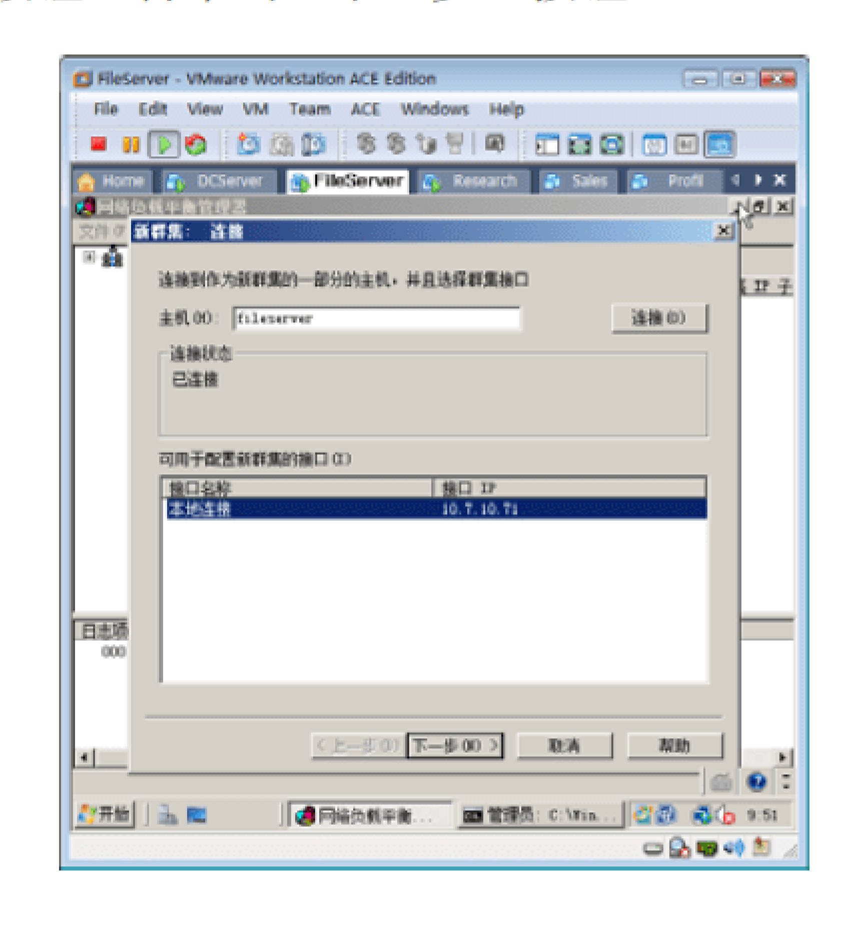


图 14-10　连接到服务器

⑦ 如图 14-11 所示，在出现的“新群集：主机参数”对话框中，优先级(单一主机标识符)选择 1，单击“添加”按钮，在对话框中输入专用 IP 地址(即配置 NLB 网卡的现在的 IP 地址)，单击“下一步”按钮。

注意：参数为每个主机指定一个唯一 ID。群集的当前成员中优先级数值最低的主机处理端口规则未涉及所有群集的网络通信。可以通过在“端口规则”选项卡中指定规则，来覆盖这些优先级或者为特定范围的端口提供负载平衡。 如果新主机加入了群集，并且其优先级与群集中的另一个主机冲突，则不能接受该主机作为群集的一部分。群集的其余部分将继续处理通信。会将描述此问题的消息写入 Windows 事件日志中。

⑧ 如图 14-12 所示，在出现的新群集对话框中，单击“添加”按钮，在出现的对话框中输入 NLB 群集 IP 地址，单击“确定”按钮。再单击“下一步”按钮。

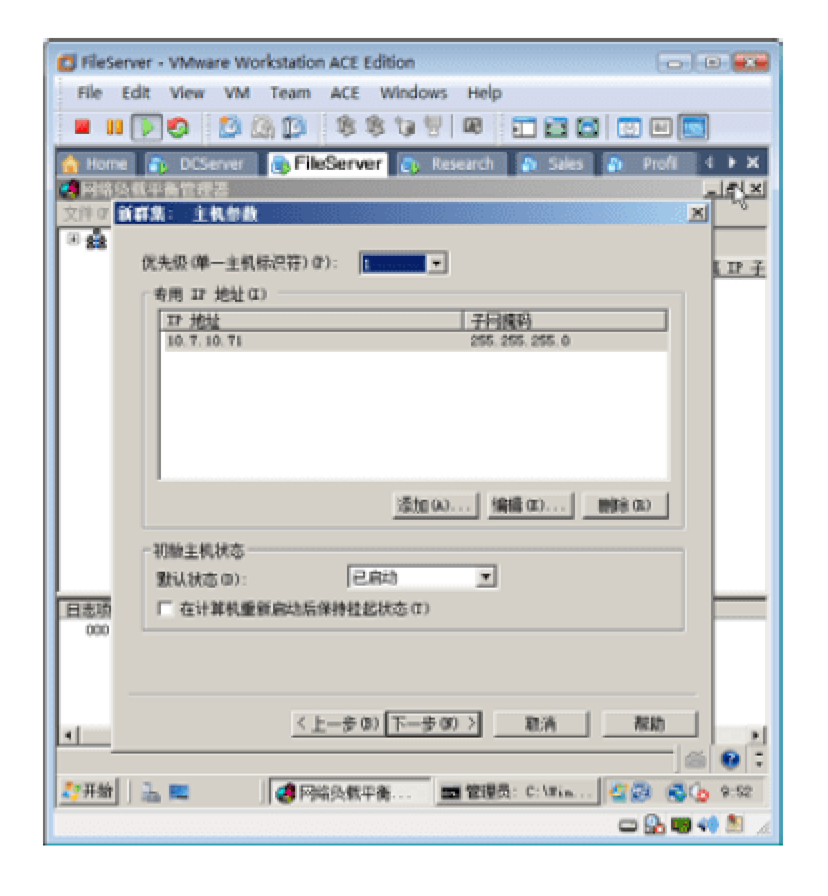


图 14-11　选择主机 ID

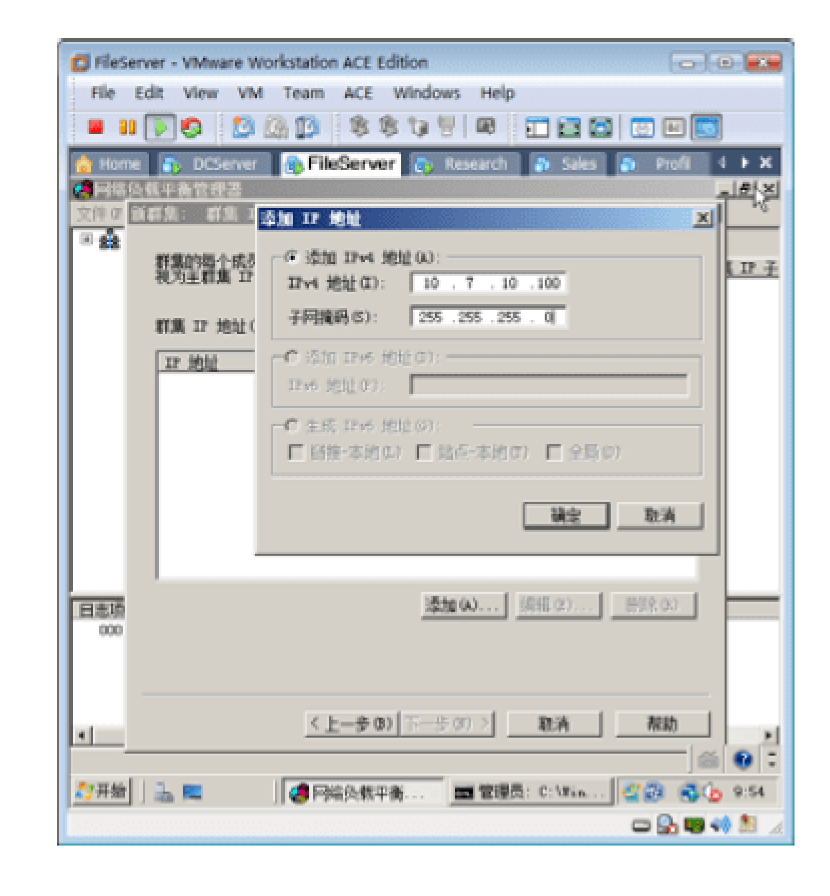


图 14-12　输入 NLB IP 地址

⑨　如图 14-13 所示，在出现的“新群集：群集参数”对话框中，输入完整的 Internet 名称。如果是 Web 站点，可以输入访问该站点的域名，群集操作模式选择“多播”单选按钮，单击“下一步”按钮。

注意：在多播模式下，实体主机之间可以互相通信。一般来说，在创建 NLB 时，可以选择单网卡多播，双网卡单播。双网卡单播时，因为主机之间不能互相通信，将设置内网通信的网卡，也就是群集设置中的心跳。微软官方推荐在 NLB 设置时，首先考虑单播模式，除非单播不能满足其要求。

⑩　如图 14-14 所示，在端口规则对话框中，单击“编辑”按钮。查看可以设置的项，保持默认，单击“完成”按钮。

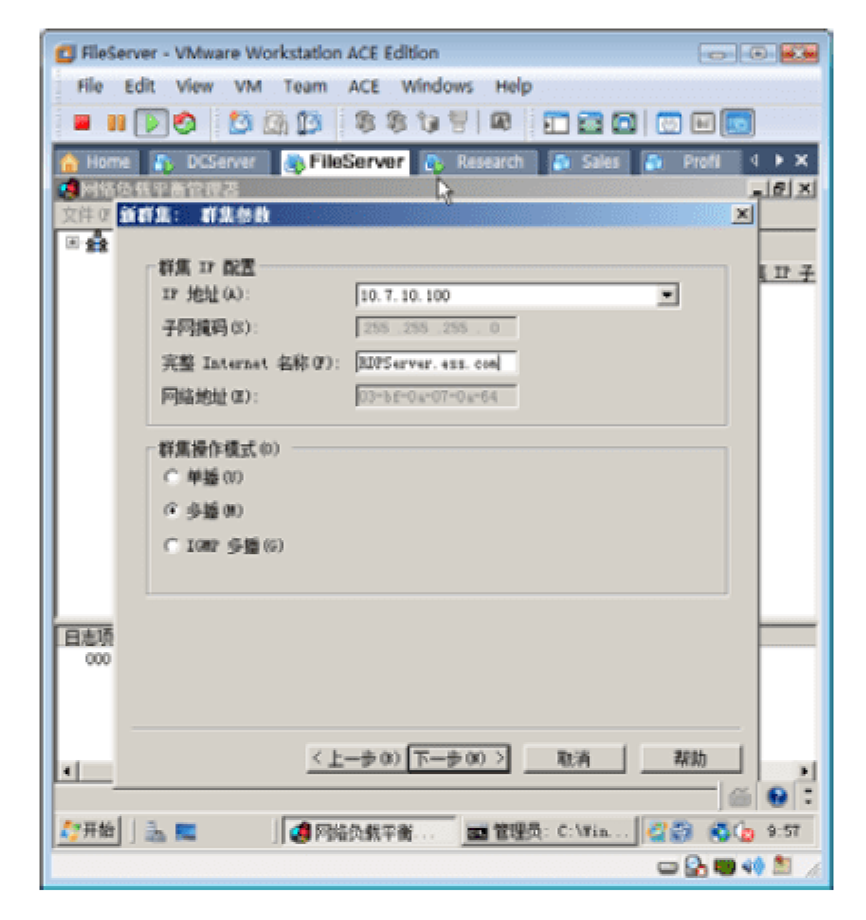




图 14-13　群集 IP 地址和域名

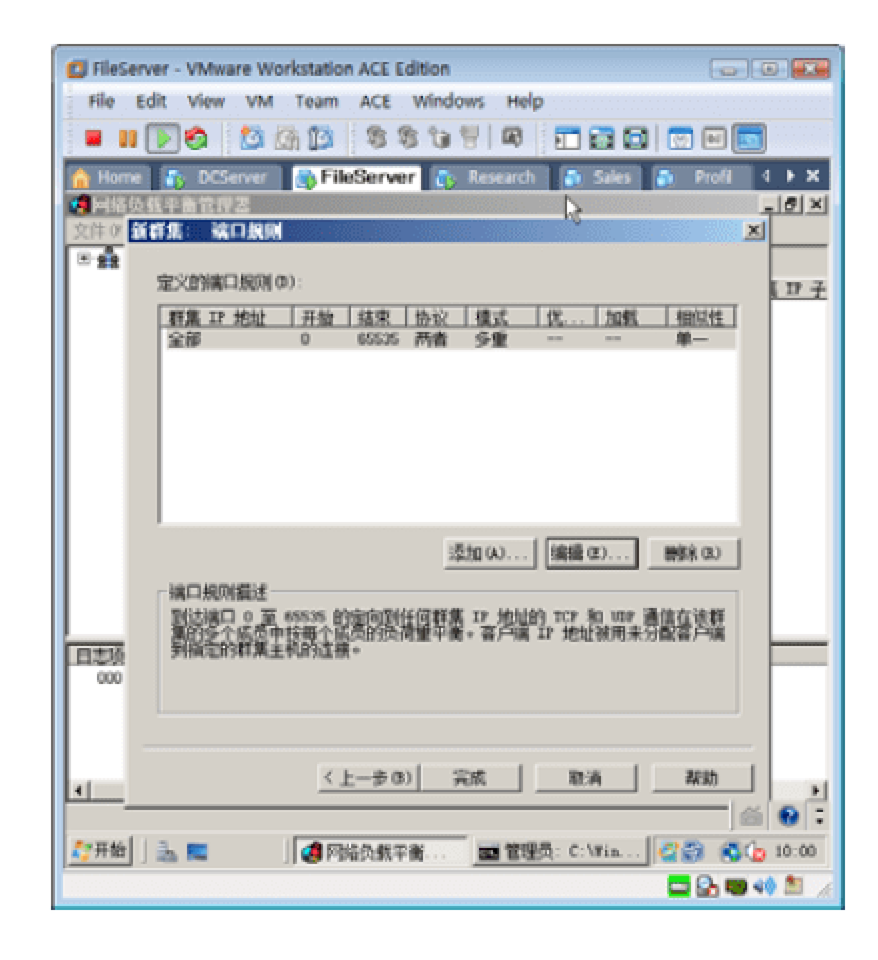


图 14-14　编辑端口规则

⑪　在端口规则对话框中，单击“编辑”按钮。如图 14-15 所示，可以“编辑”端口规则。在筛选模式下，选中“无”单选按钮，单击“确定”按钮。

端口规则，可以指定在哪些端口上和协议上实现网络负载平衡。比如 Web 站点的负载平衡，就可以选择 TCP 的 80 端口。

- 筛选模式“多个主机”参数：指定群集中的多个主机将针对关联的端口规则处理网络通信。该筛选模式通过将网络负载分发在多个主机中来提供缩放的性能和容错。用户可以指定在各个主机中同等分发负载，或者每个主机处理指定的负载权重。
- “单一主机”参数：指定由群集中的单个主机根据指定的处理优先级处理针对关联端口规则的网络通信。该筛选模式提供端口特定的容错来处理网络通信。
- “禁用此端口范围”参数：指定阻止针对关联端口规则的所有网络通信。在这种情况下，NLB 驱动程序将筛选所有相应的网络数据包或数据报。该筛选模式允许阻止地址为特定端口范围的网络通信。
- “相似性”参数：仅适用于“多个主机”筛选模式。
- “无”选项：指定来自相同客户端 IP 地址的多个连接可以由不同的群集主机进行处理(没有客户端关联)。为了使网络负载平衡能够正确处理 IP 分段，选择 UDP 或“两者”作为协议设置时，应该避免使用“无”。
- “单一”选项：指定 NLB 应该将来自相同客户端 IP 地址的多个请求引导至同一个客户端主机。

这是“相似性”的默认设置。还可以通过启用“网络”选项来代替“单个”选项，修改 NLB 客户端关联，以便将来自 TCP/IP 的 C 类地址范围(而不是单个 IP 地址)的所有客户端请求引导至单个群集主机。该功能确保使用多个代理服务器访问群集的客户端可以使其 TCP 连接指向同一个群集主机。

■ “网络”选项：指定 NLB 应该将来自相同 TCP/IP 的 C 类地址范围的多个请求引导至同一个客户端主机。启用“网络”关联，而不是启用“单个”关联，可确保使用多个代理服务器访问群集的客户端能够使其 TCP 连接指向同一个群集主机。

在客户端站点上使用多个代理服务器会导致来自单个客户端的请求显示为来自不同的计算机。如果所有客户端的代理服务器都位于同一个地址范围内，则“网络”关联会确保正确处理客户端会话。如果不需要该功能，请使用“单个”关联以最大限度地提高缩放性能。

⑫ 完成配置。

⑬ 如图 14-16 所示，在命令提示符下输入 ipconfig，可以看到添加的 NLB IP 为 10.7.10.100。

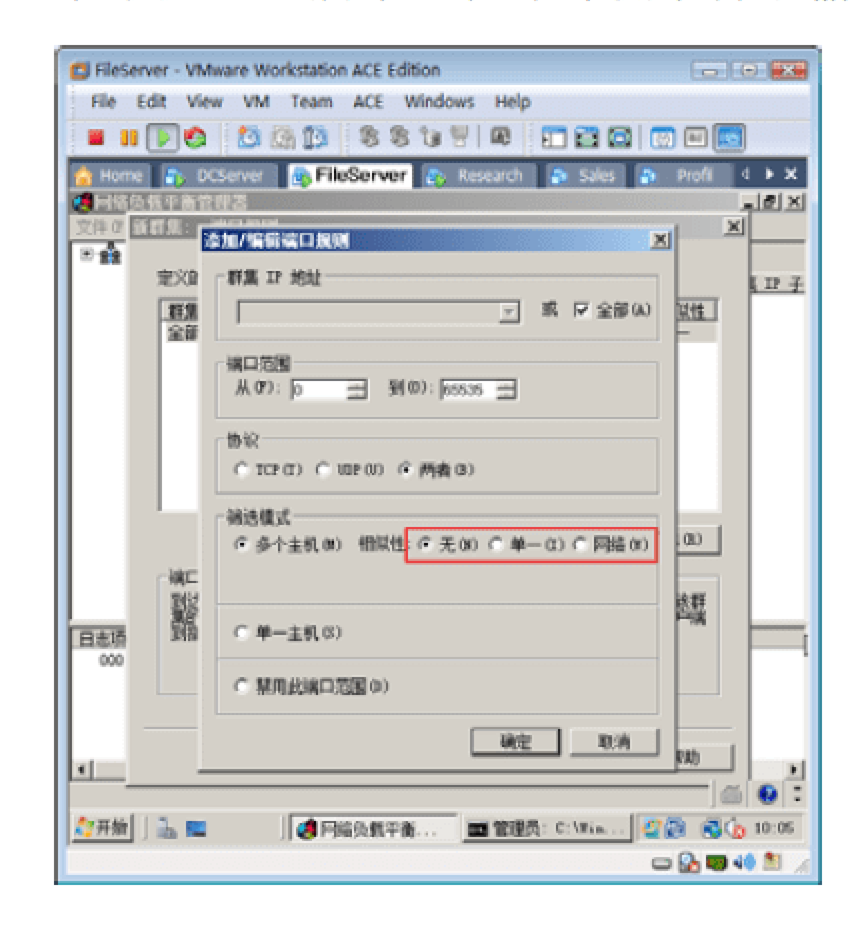


图 14-15 配置筛选模式

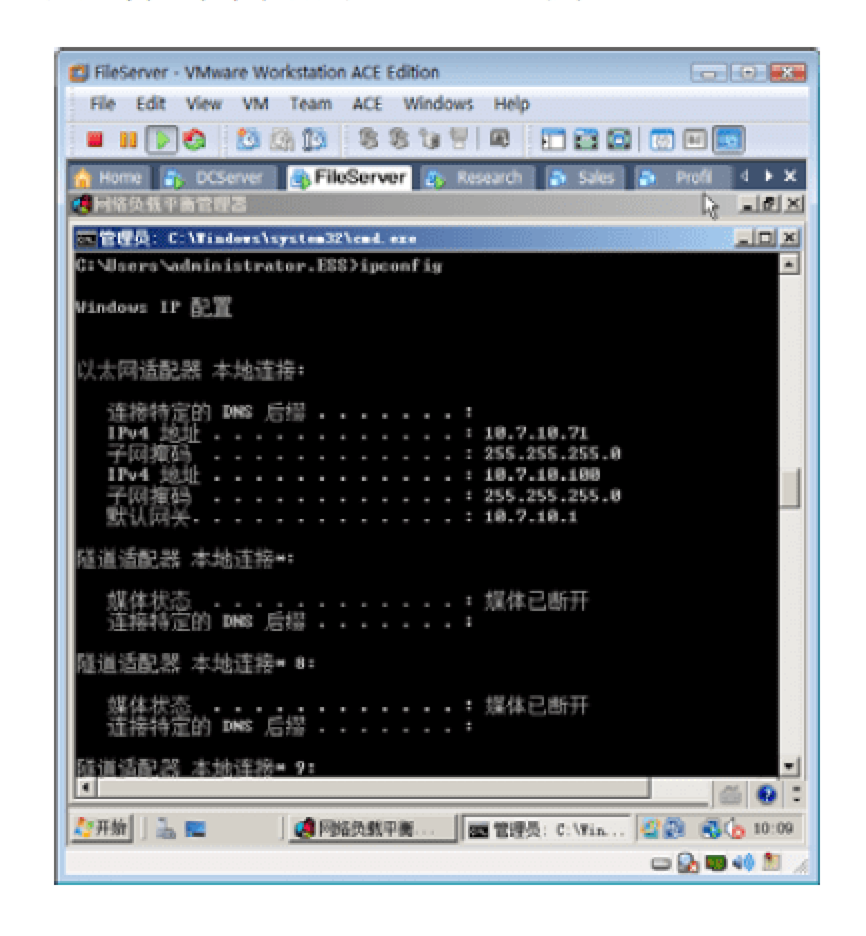


图 14-16 查看 NLB 地址

⑭ 如图 14-17 所示，右击刚才创建的群集，从弹出的快捷菜单中选择“添加主机到群集”命令。

⑮ 如图 14-18 所示，输入 research 地址，单击“连接”按钮，再单击“下一步”按钮。

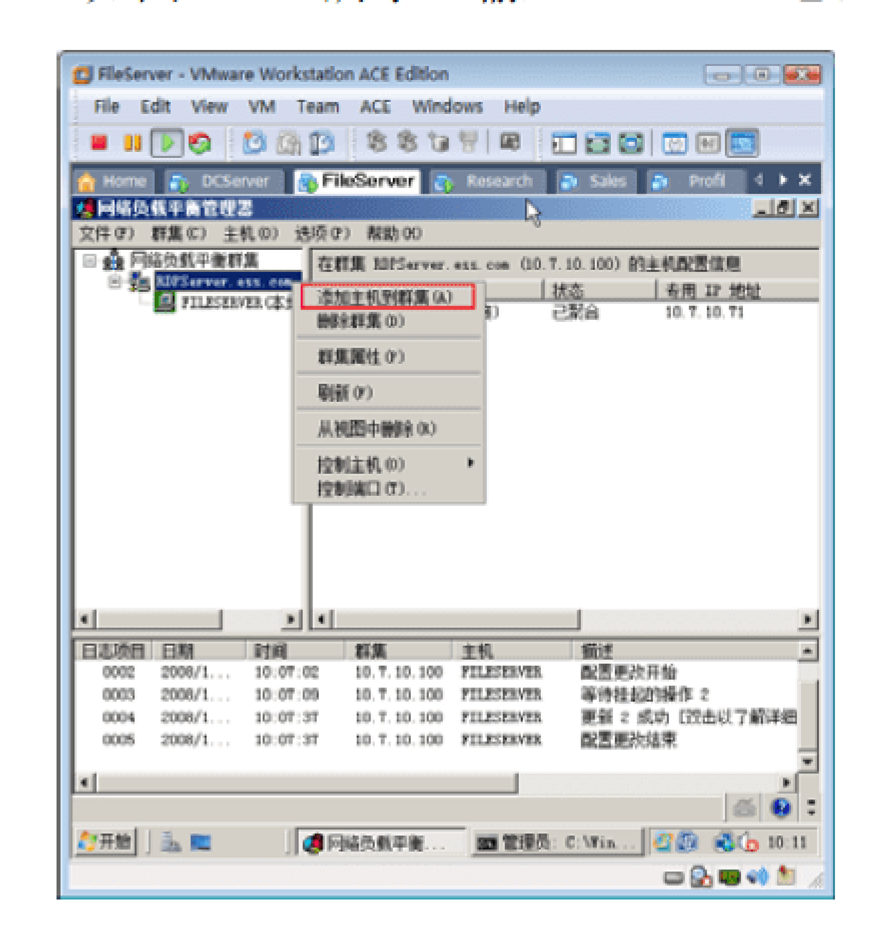


图 14-17 添加主机到群集

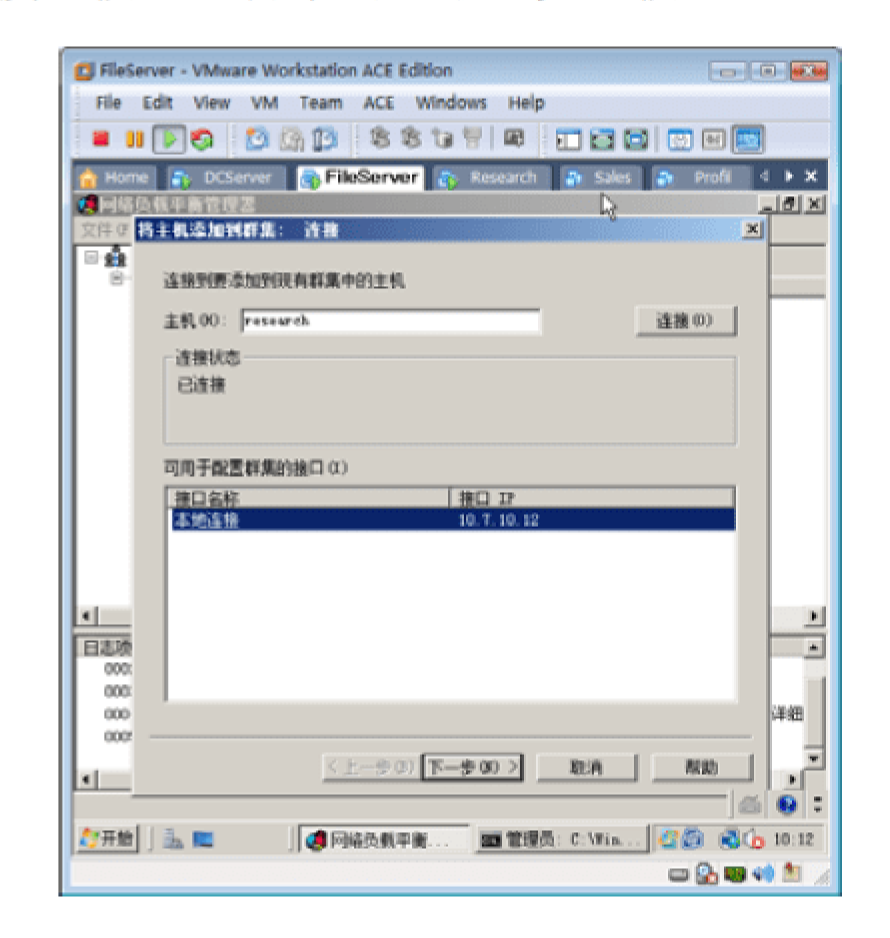


图 14-18 连接到主机

⑯　如图 14-19 所示，在出现的主机参数对话框中，优先级默认就是 2，单击“下一步”按钮。



提示：如果提示没有权限，需要使用域管理员账户在 FileServer 上登录，如果 FileServer 和 Research 属于工作组，再更改 FileServer 管理员的账号和密码与 Research 计算机上的管理员账号和密码一致。如果连接不成功，需要关闭 Research 的防火墙。

⑰　如图 14-20 所示，在出现的端口规则对话框中，保持默认设置，单击“完成”按钮。

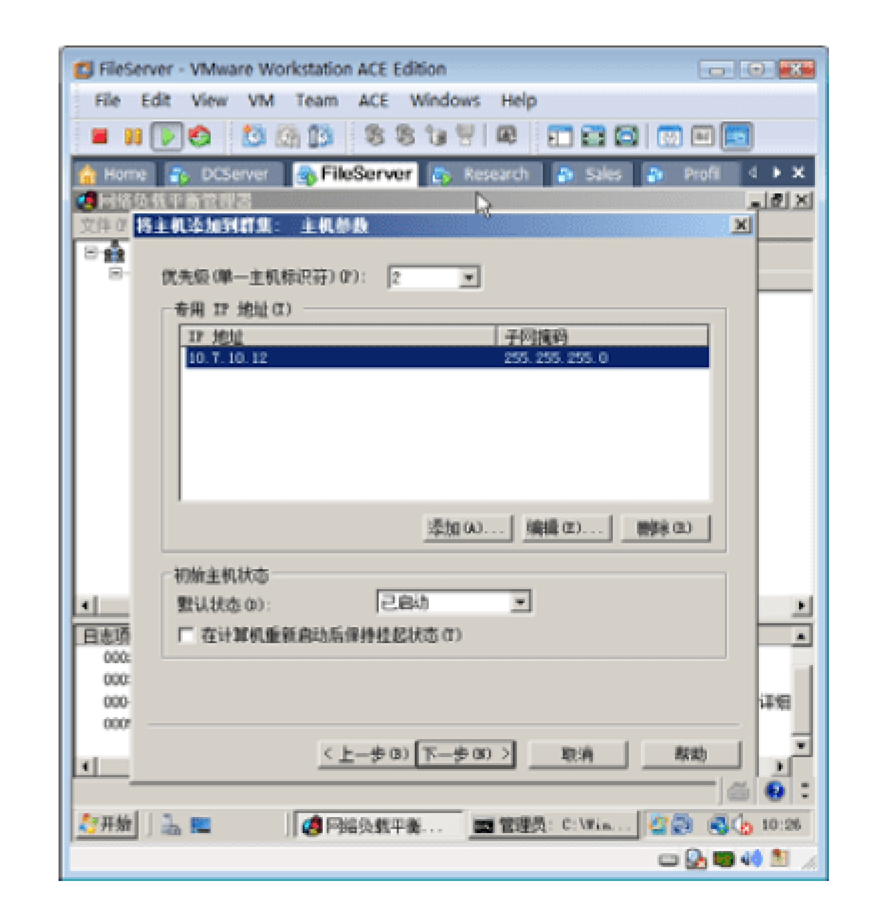



图 14-19　主机标识符

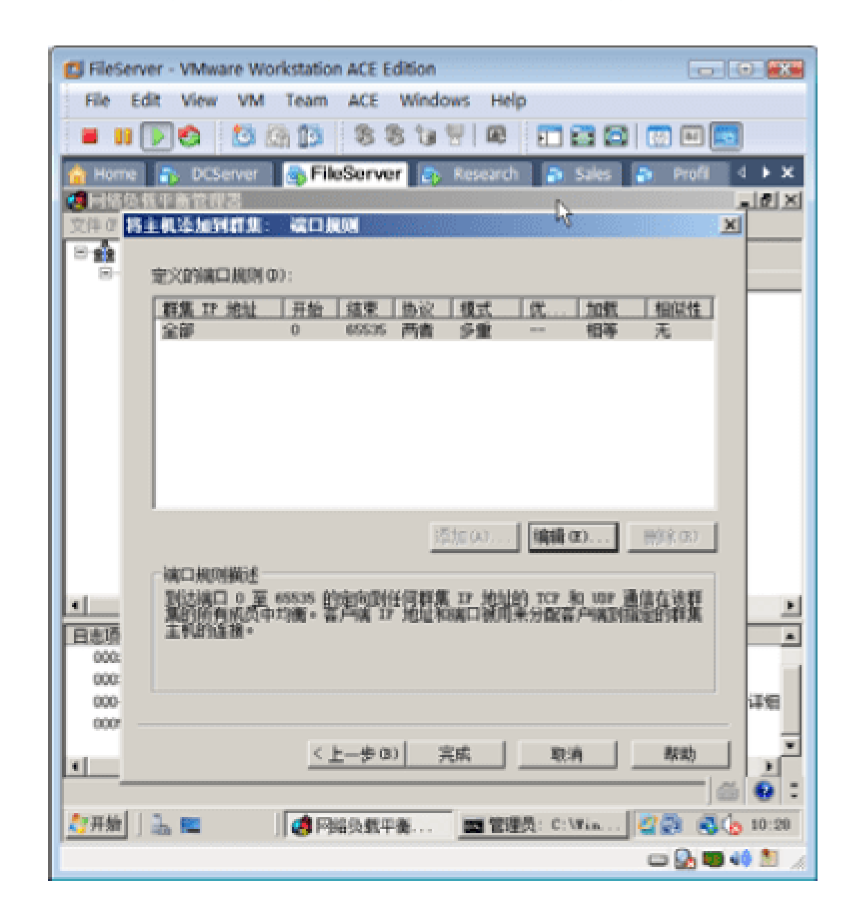


图 14-20　端口规则

⑱　如图 14-21 所示，过一段时间，群集中的两个节点都变成已聚合状态，说明配置成功。

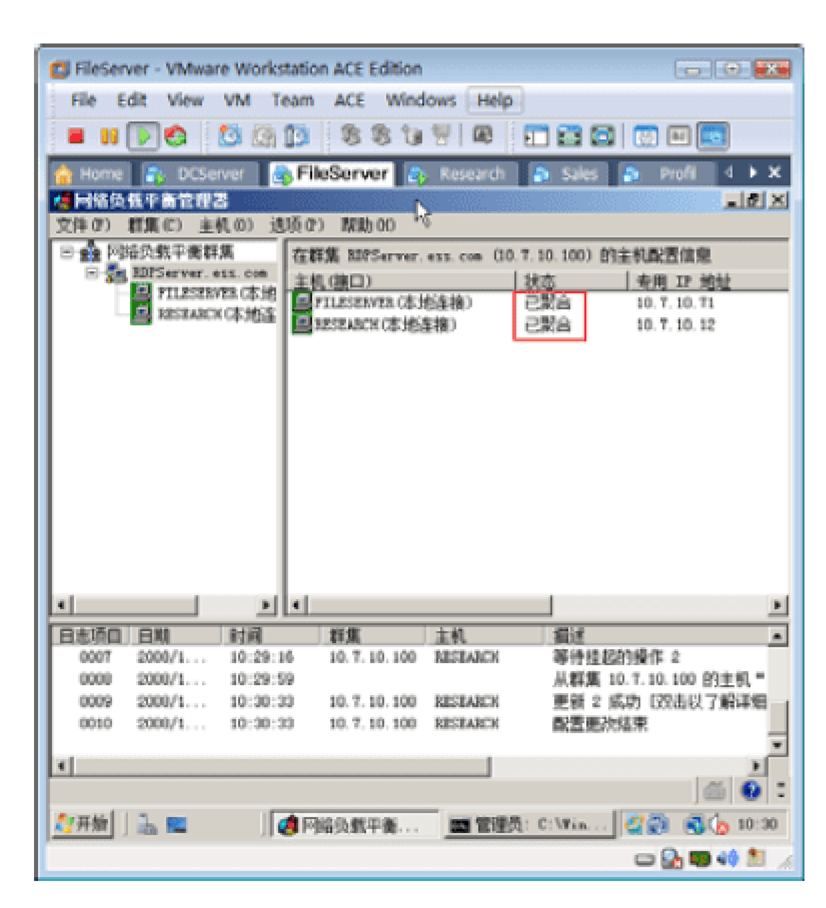


图 14-21　聚合

14.3.2　验证网络负载平衡

下面介绍使用远程桌面验证 NLB 的配置。

①　在 Sales 计算机上，选择“开始”→“运行”命令，在出现的“运行”对话框中输入 mstsc，单击“确定”按钮，打开远程桌面客户端。

②　连接 10.7.10.100，输入账号和密码。

③ 再次运行 mstsc，输入 10.7.10.100，输入账号和密码，可以看到连到了不同的服务器，如图 14-22 所示。可以说明已经实现网络负载平衡。

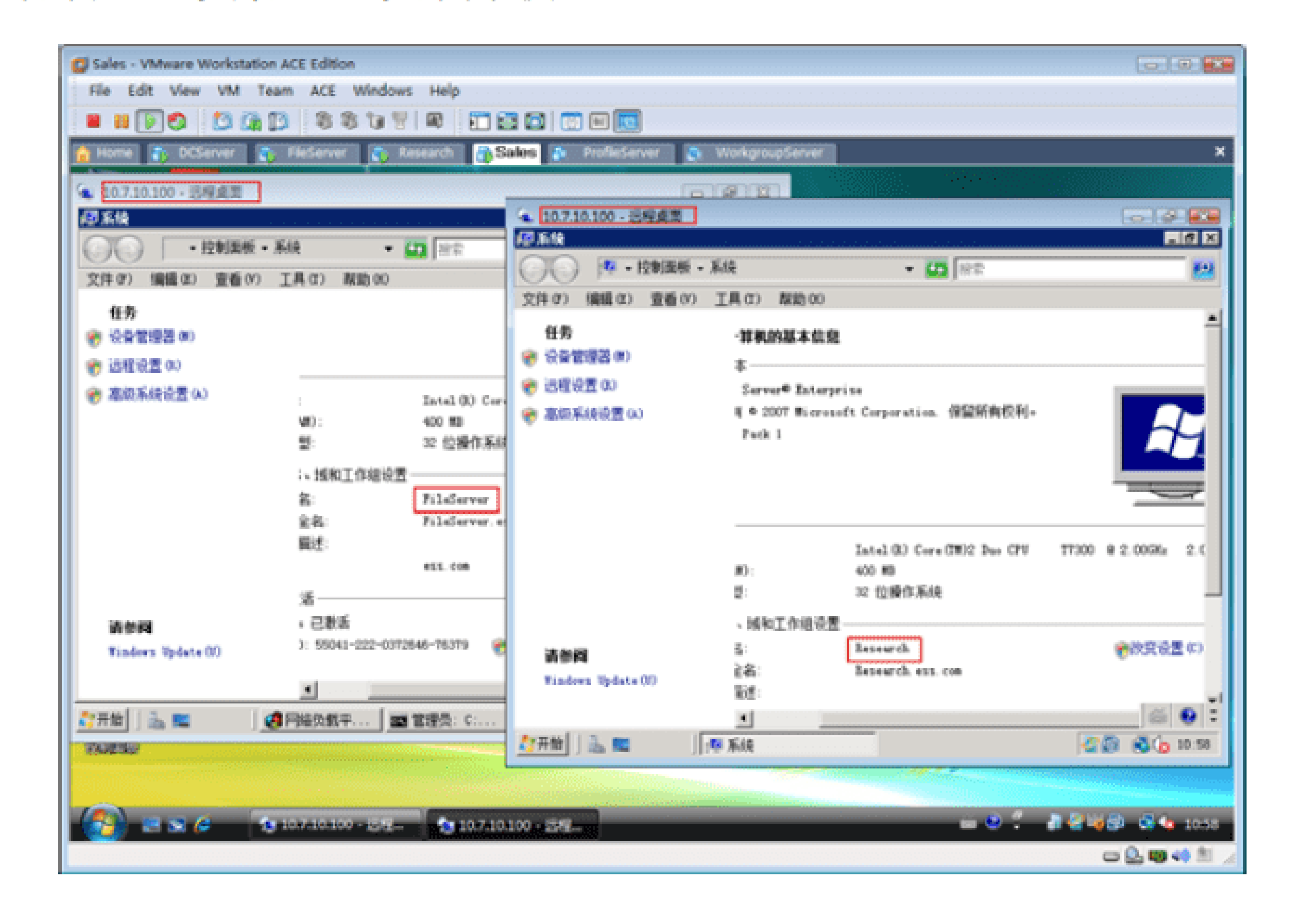


图 14-22 网络负载平衡确认

④ 如图 14-23 所示，断开 FileServer 的网络连接。

⑤ 如图 14-24 所示，在 Sales 计算机上使用远程桌面连接 10.7.10.100。可以发现将用户定位到了 Research 服务器。

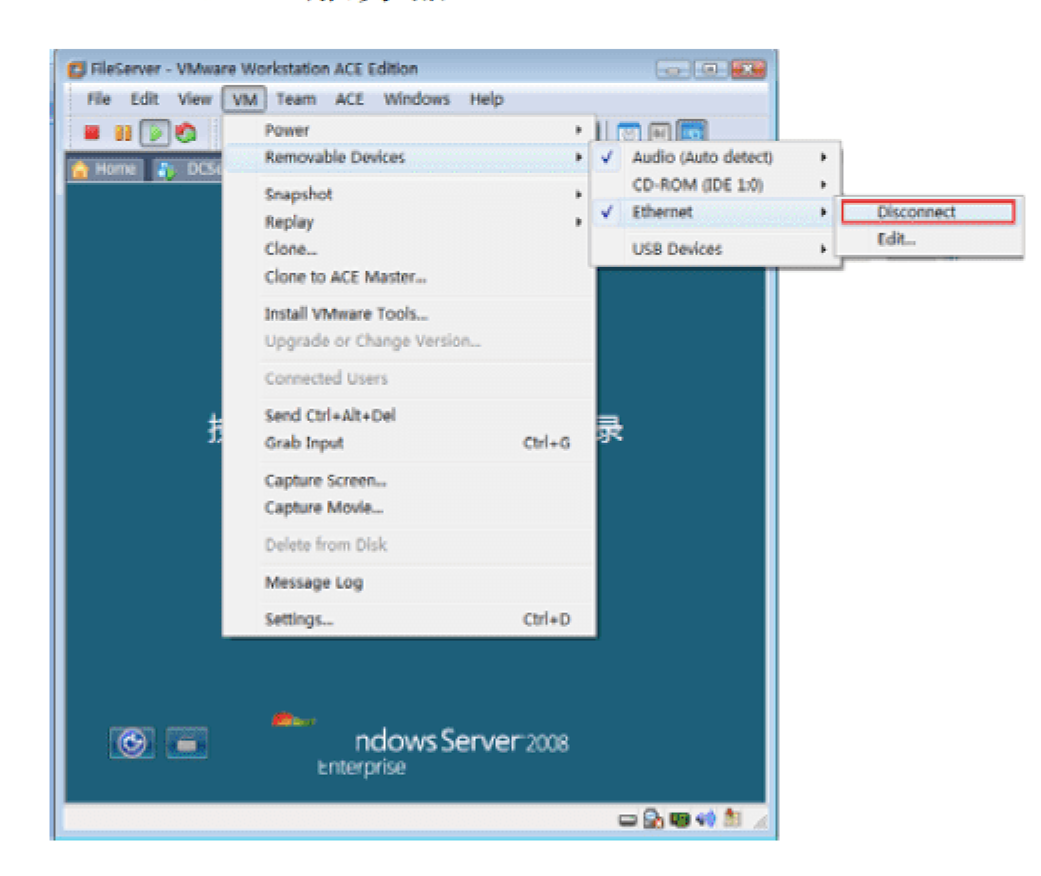


图 14-23 断开网络连接

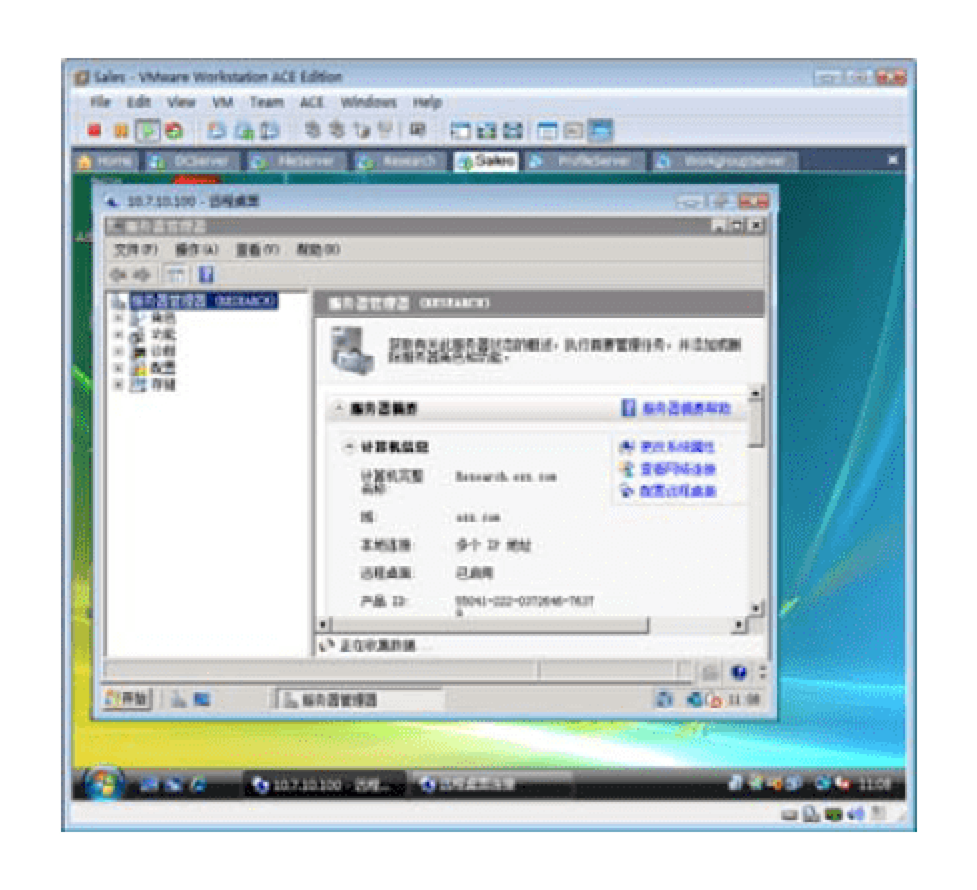


图 14-24 验证 NLB

⑥ 断开 Research 服务器的网络，将 FileServer 网络连接上，在 Sales 计算机上使用远程桌面连接 10.7.10.100，可以发现将用户定位到了 FileServer。这证明 NLB 还可以实现容错。

14.4 QoS

QoS 的英文全称为 Quality of Service，中文名为“服务质量”。QoS 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或

E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不被延迟或丢弃，同时保证网络的高效运行。

在 Windows 中，基于策略的 QoS 结合了基于标准的 QoS 的功能性和组策略的可管理性。此组合使 QoS 策略更易于应用到组策略对象中。Windows 包括一个基于策略的 QoS 向导，可帮助用户在组策略中配置 QoS。

示例：使用 QoS 限制从文件服务器下载带宽

1. 实验环境

FileServer 安装有 Windows Server 2008 企业版。

Sales 安装有 Vista 企业版。

实验示意图如图 14-25 所示。

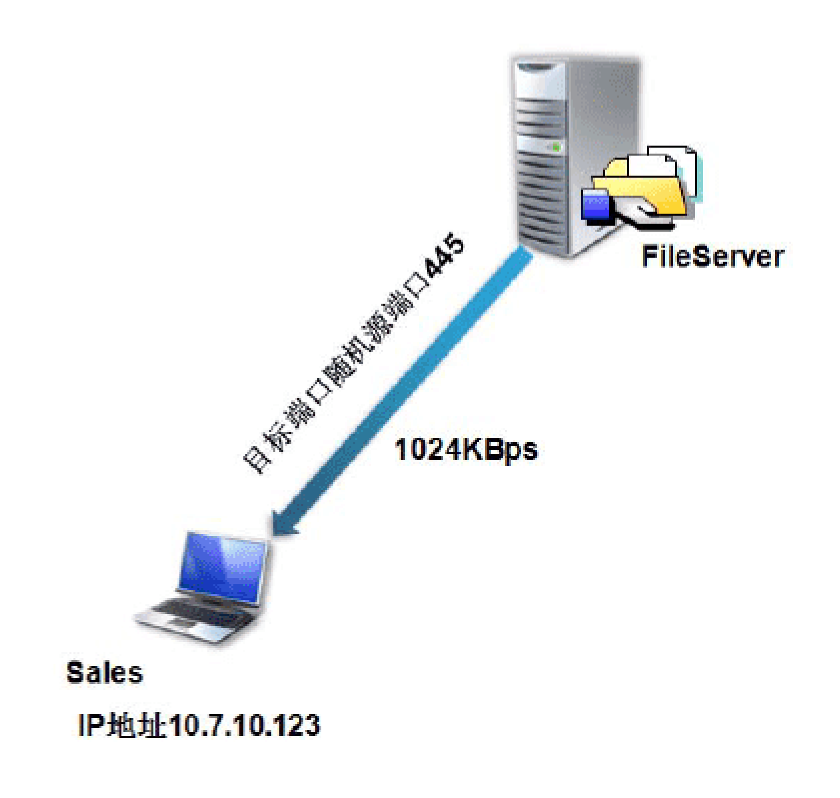


图 14-25　实验示意图

2. 实验目标

限制 Sales 计算机从 FileServer 服务器上下载文件的带宽。

使用性能计数器检测比较使用 QoS 策略前后复制文件时的带宽。

以下操作将创建 QoS 规则，用它来演示如何管理服务质量的内在功能。将创建基于策略的 QoS 规则，该规则的作用是将传输至特定计算机端口 445 的流量限制到 1024 KB/s。此策略仅供演示之用。在使用网络资源时，全局性地限制端口 445 可能会造成严重的性能损失。此外，此任务还将通信限制到特定的 IP 地址。在实际部署中，可以将部署限制到一组 IP 地址(如子网)，这通过输入子网 ID，用它来代替单一 IP 地址即可实现。

① 在 FileServer 上，选择“开始”→“运行”命令，在出现的“运行”对话框中输入 MMC，单击“确定”按钮。

② 如图 14-26 所示，在打开的微软管理控制台中，选择“文件”→“添加/删除管理单元”命令。

③ 如图 14-27 所示，在“添加或删除管理单元”对话框中，选择“可靠性和性能监视器”，单击“添加”按钮，然后单击“确定”按钮。

④ 如图 14-28 所示，单击按钮，添加性能计数器。

⑤ 如图 14-29 所示，在出现的“添加计数器”对话框中，选择 Network Interface 下面的 Bytes Total/sec

选项，单击“添加”按钮。

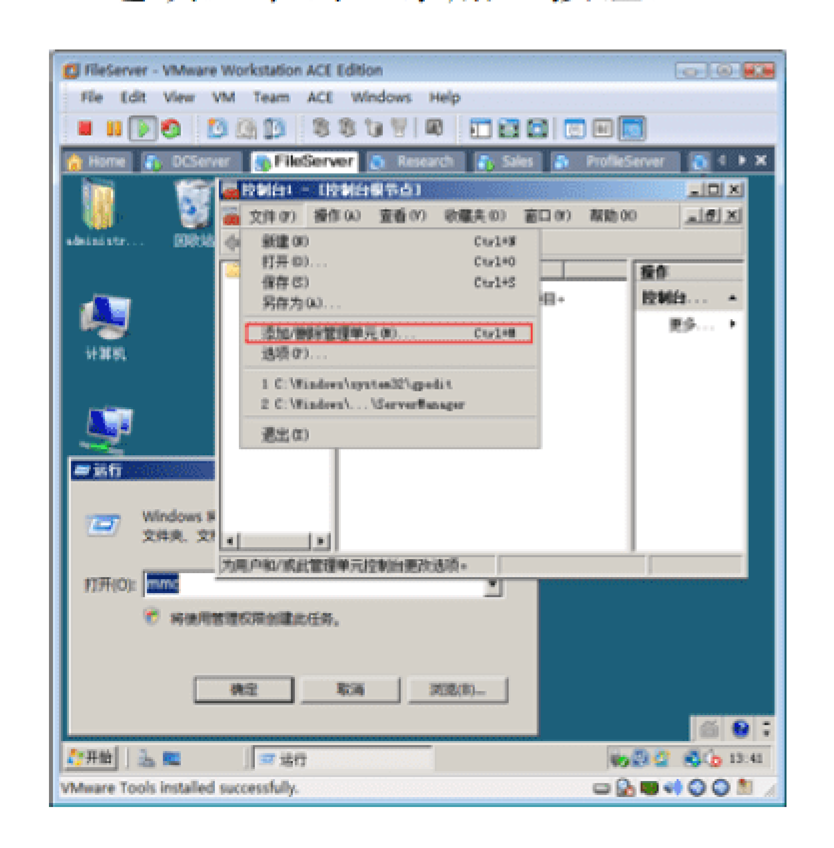


图 14-26　添加/删除管理单元

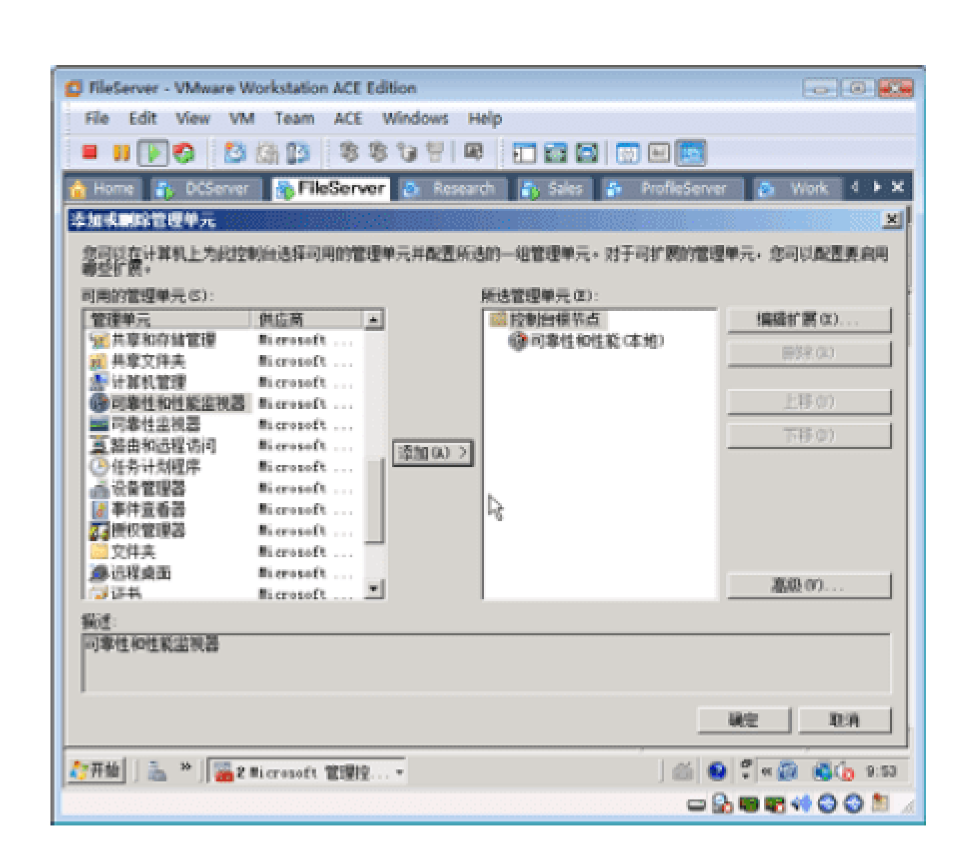


图 14-27　添加可靠性和性能监视器

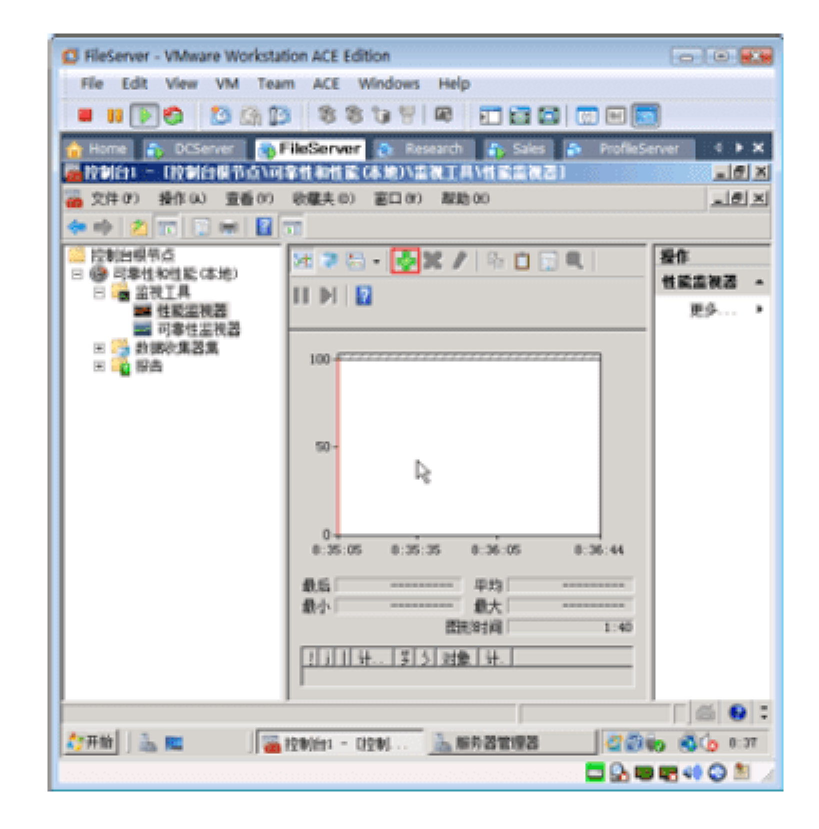


图 14-28　添加性能计数器

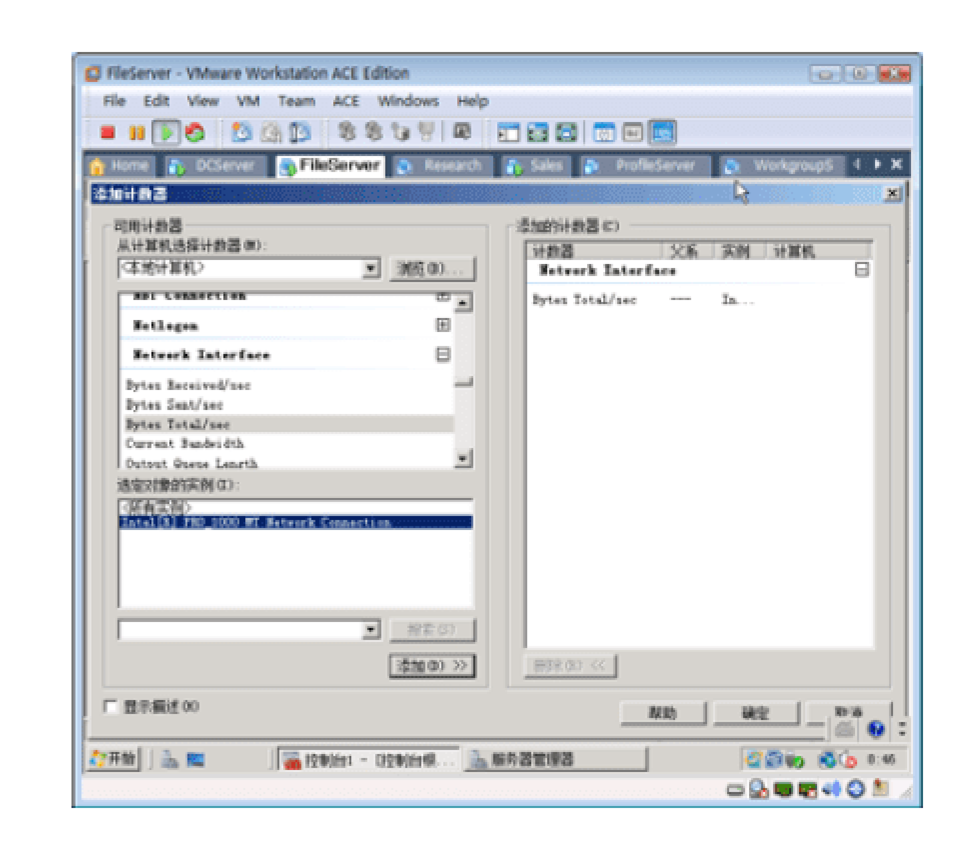


图 14-29　网络流量

⑥　如图 14-30 所示，在 Sales 计算机上访问 FileServer 共享文件，将其中的一个电影文件复制到 Sales 桌面上，单击⊙按钮。

⑦　如图 14-31 所示，可以看到复制文件的速度。

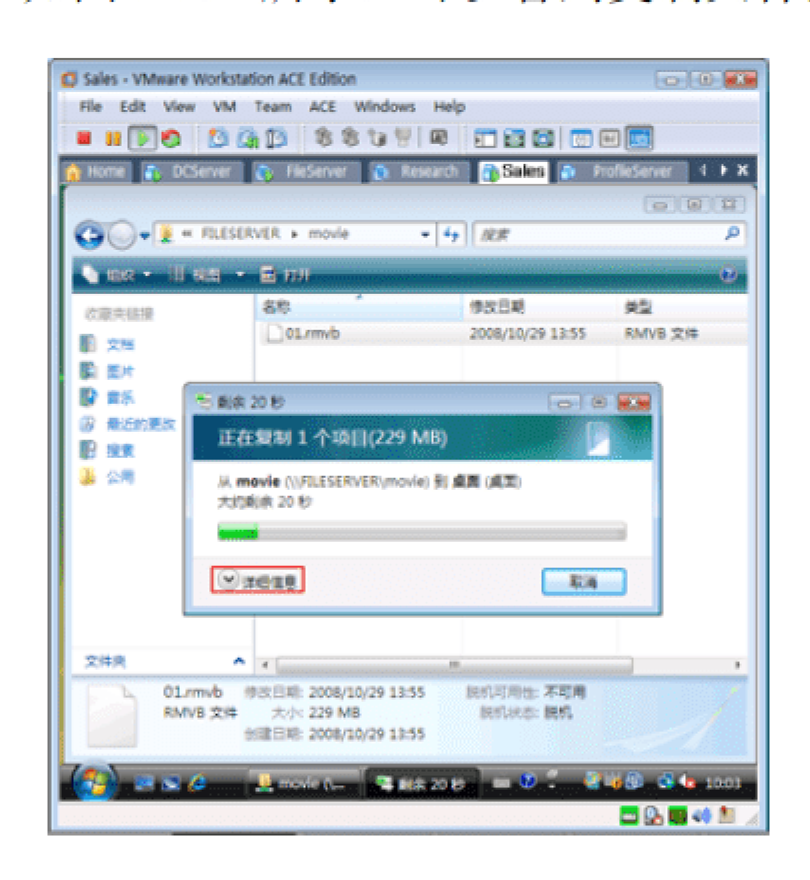


图 14-30　复制文件

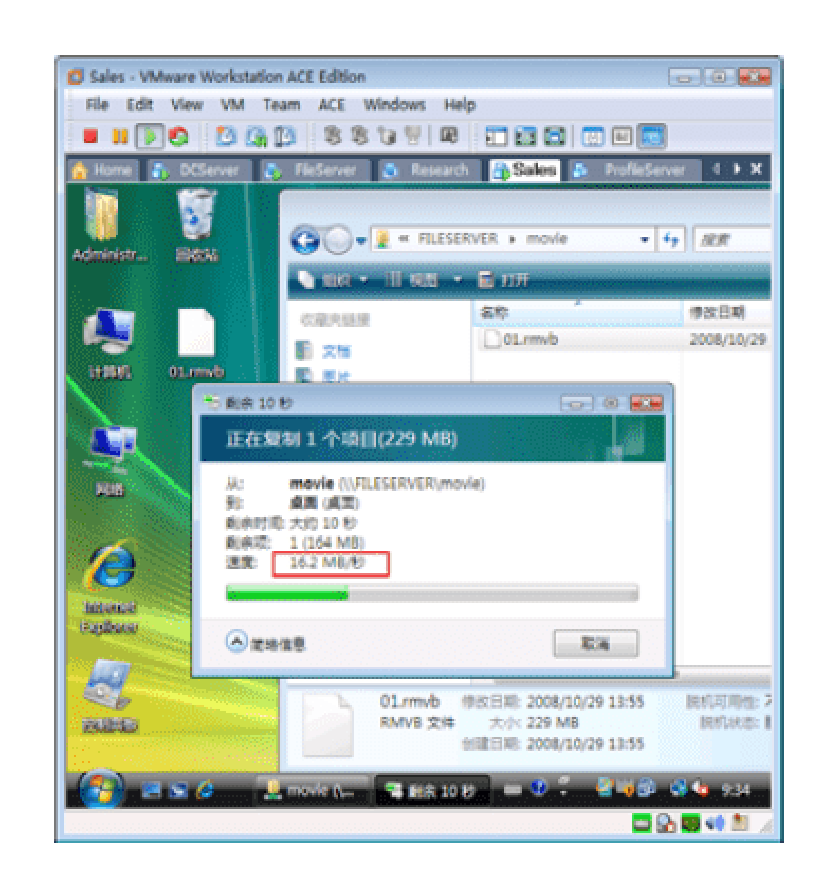


图 14-31　查看流量

⑧ 如图 14-32 所示，在 FileServer 上，打开性能监视器，单击按钮，选择“报告”，可以看到以数字显示的带宽，如图 14-33 所示。



提示： 可以看到在没有限制带宽使用的情况下，复制文件将尽可能地使用网络带宽。以下操作将会创建基于策略的 QoS。

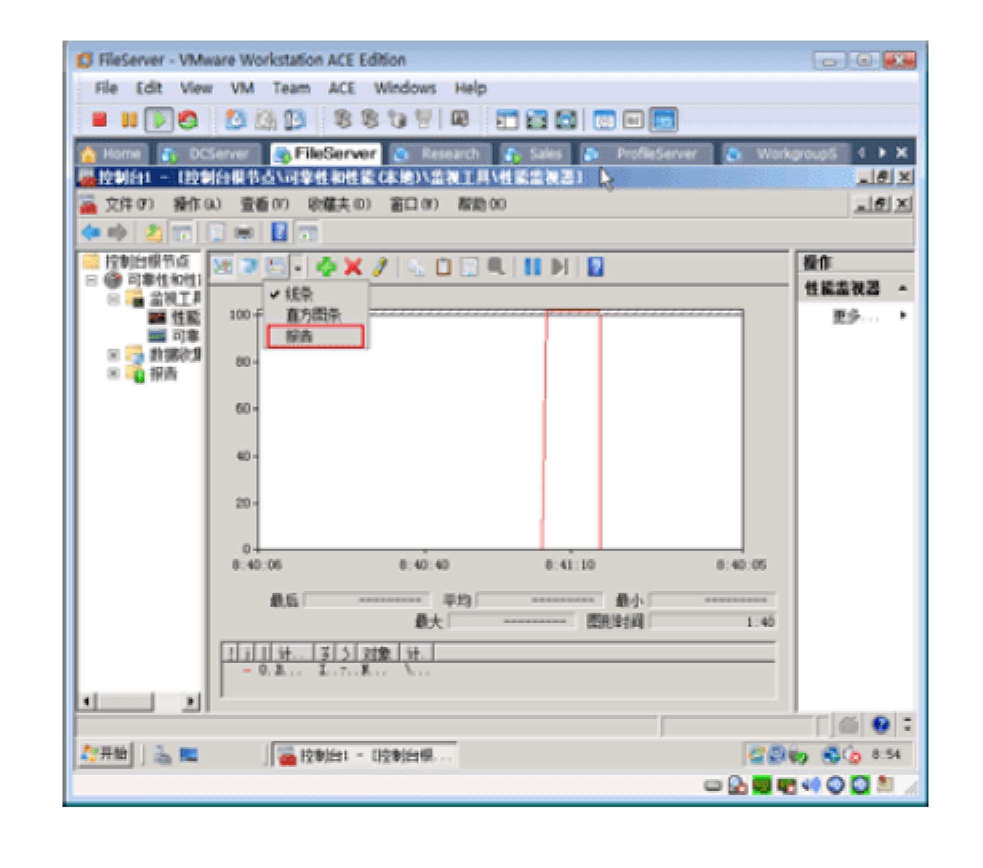


图 14-32　改变显示方式

图 14-33　显示带宽

⑨ 如图 14-34 所示，选择“开始”→“运行”命令，在出现的“运行”对话框中输入 gpedit.msc，单击“确定”按钮。

⑩ 如图 14-35 所示，在打开的“本地组策略编辑器”窗口中，右击“基于策略的 Qos”选项，在弹出的快捷菜单中选择“新建策略”命令。

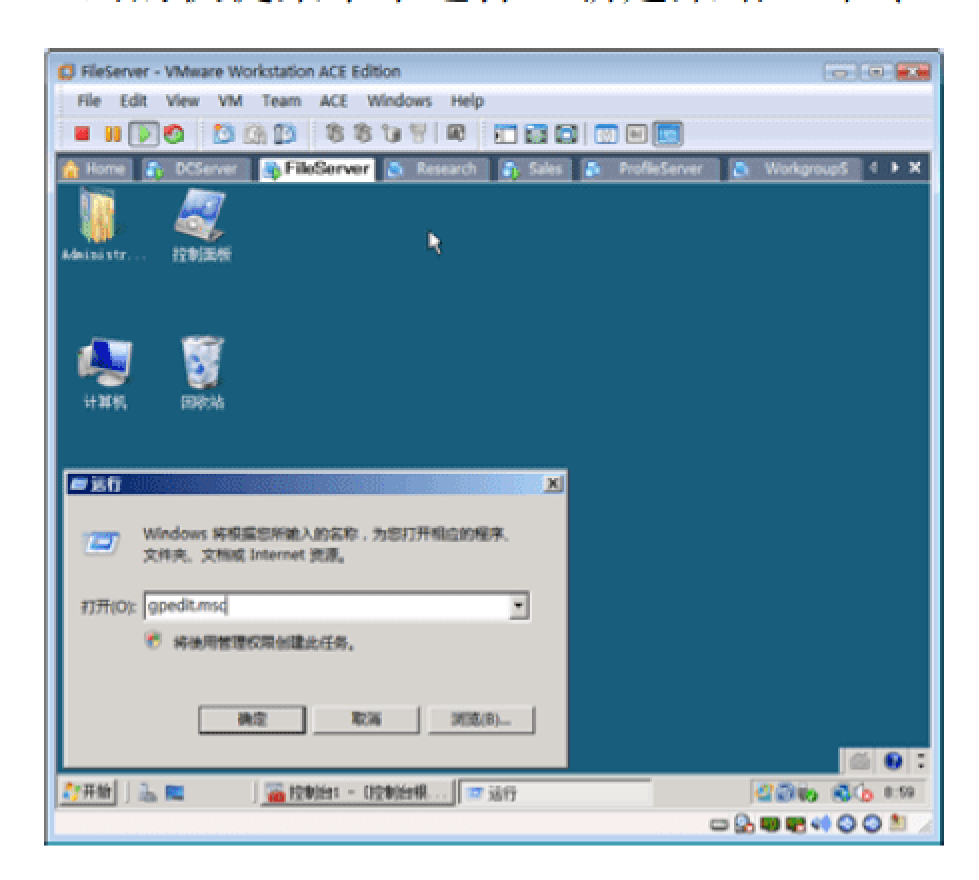


图 14-34　打开组策略编辑器

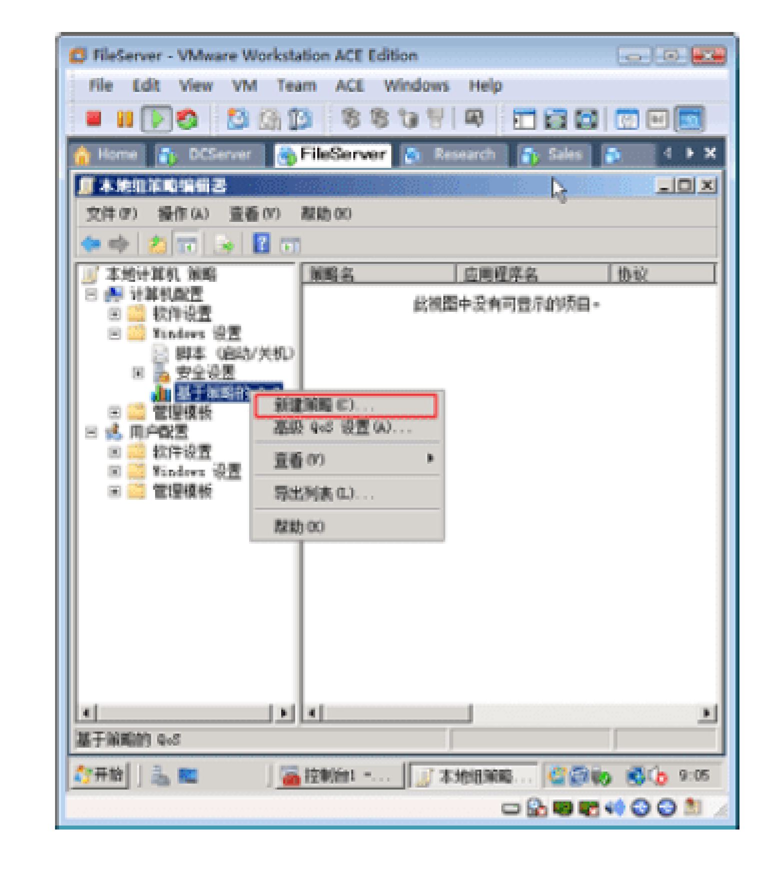


图 14-35　创建策略

⑪ 如图 14-36 所示，输入策略名称，取消选中“指定 DSCP 值”复选框，选中“指定中止值等级”复选框，输入带宽 1024，单击“下一步”按钮。

⑫ 如图 14-37 所示，选中“所有应用程序”单选按钮，单击“下一步”按钮。

⑬ 如图 14-38 所示，选中“仅用于以下目标 IP 地址或前缀”单选按钮，输入 Sales 计算机的 IP 地址。

⑭ 如图 14-39 所示，选择 TCP 协议，选中“来自此源端口号或范围”单选按钮，输入 445，单击“完成”按钮。

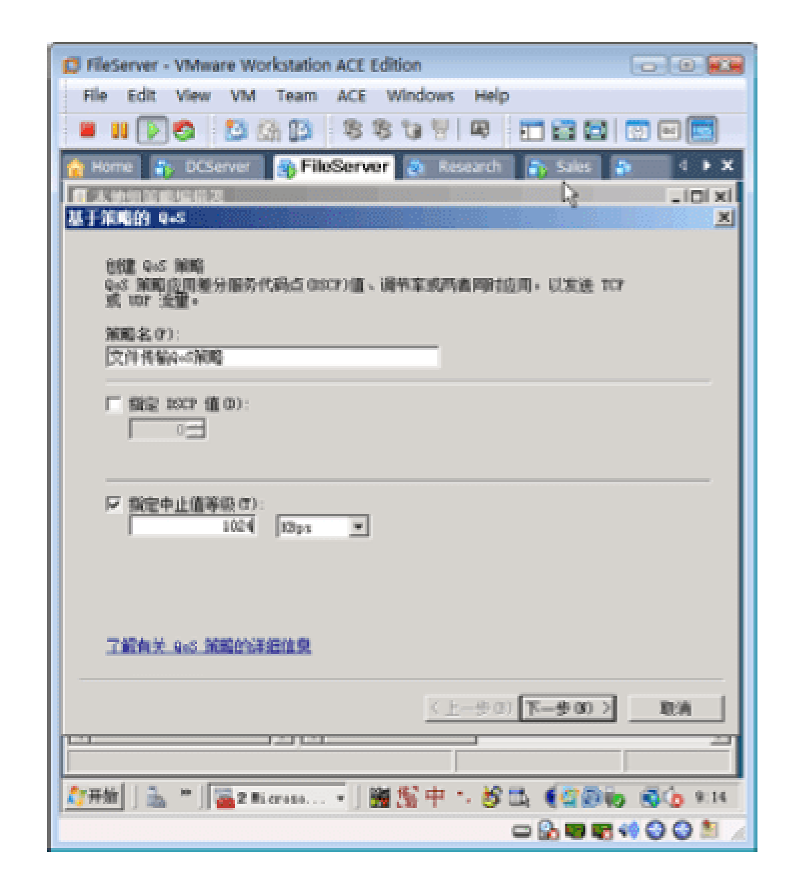


图 14-36　输入策略名称和等级

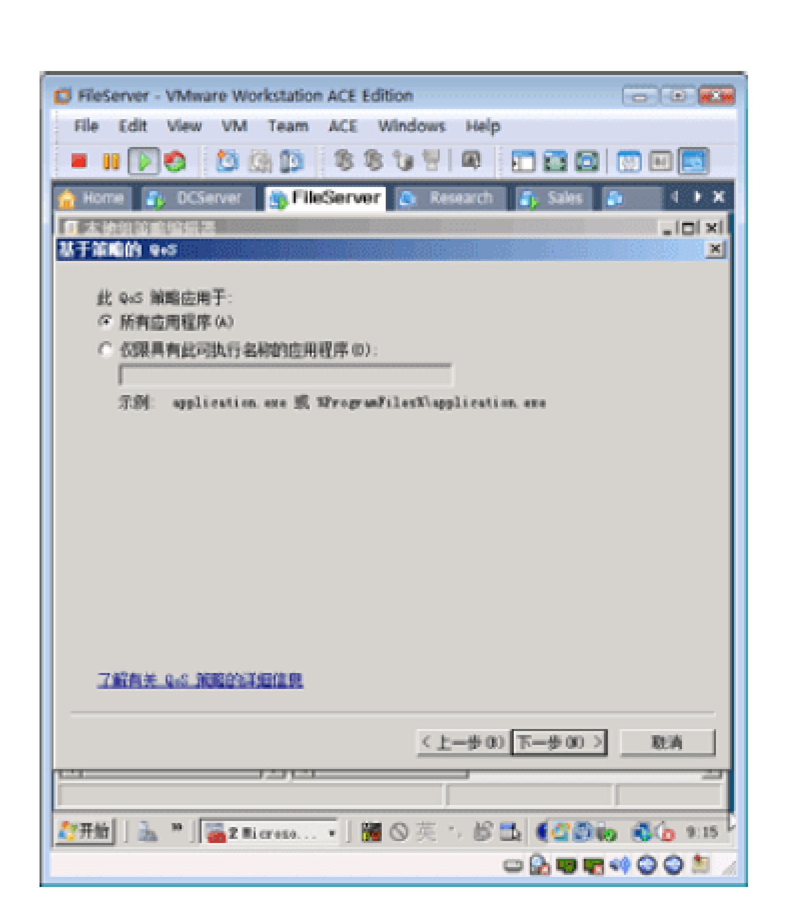


图 14-37　应用于所有程序

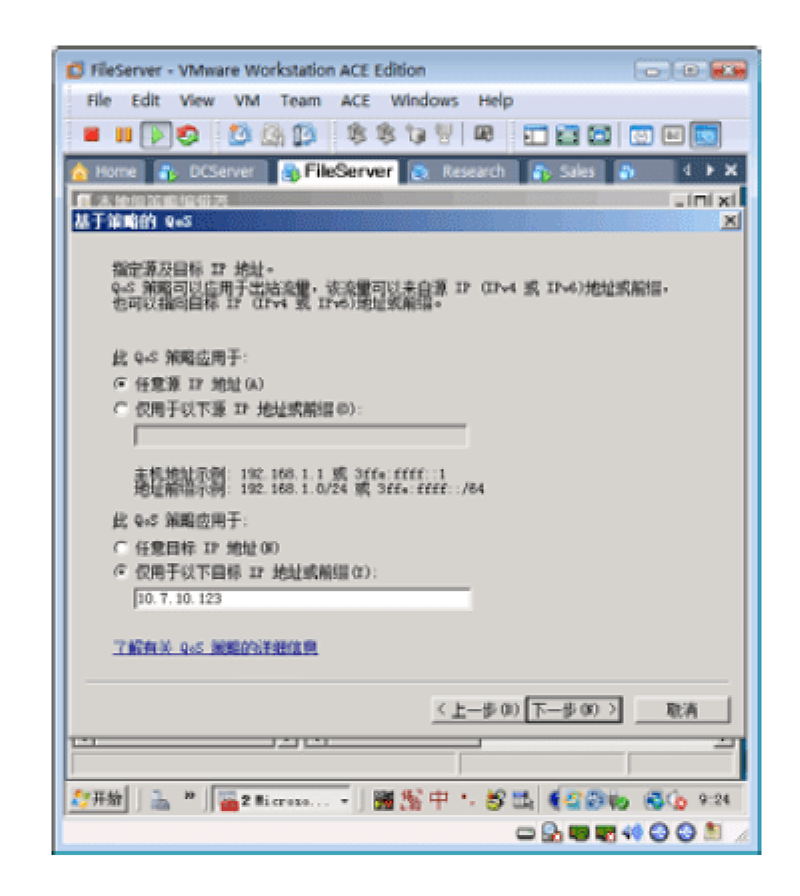


图 14-38　指定源地址和目标地址

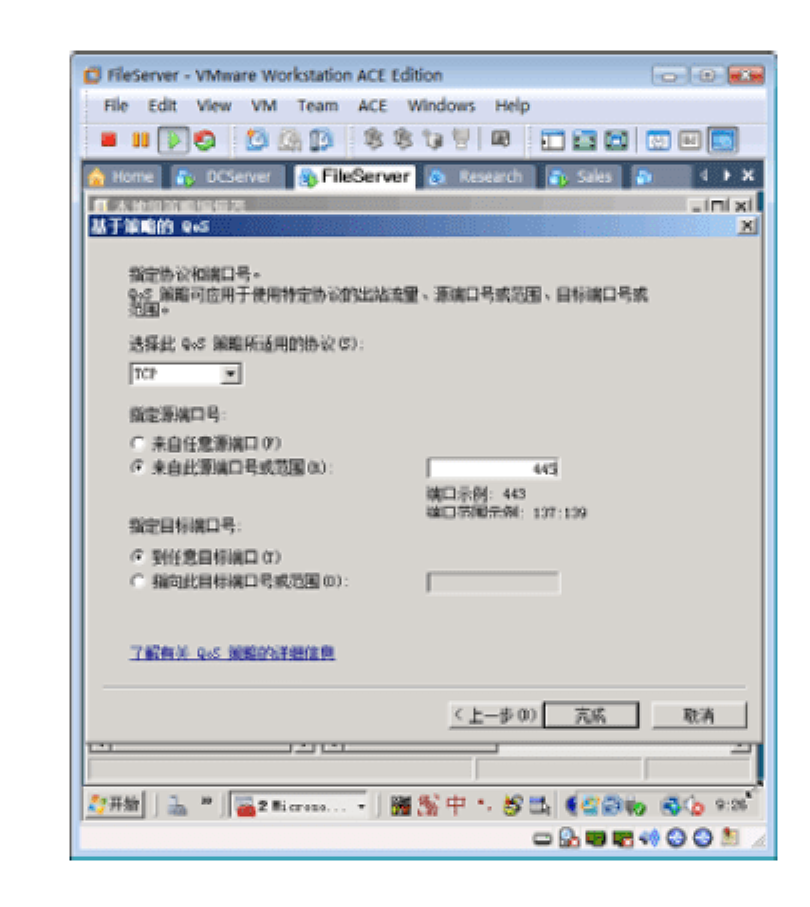


图 14-39　指定协议和端口

⑮ 如图 14-40 所示，在 Sales 上复制 FileServer 共享文件夹中的文件，可以看到传输速度被限制到 1024 KB/s 以下。

⑯ 如图 14-41 所示，在 FileServer 的性能计数器中，可以看到详细的传输速率。这说明刚才创建的限制文件传输 QoS 策略已经起作用了。

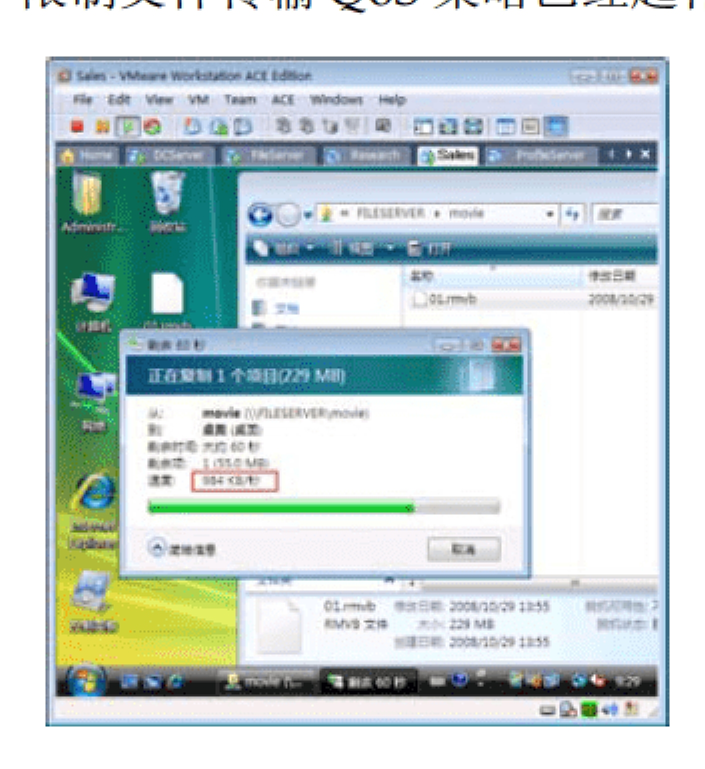


图 14-40　测试流量

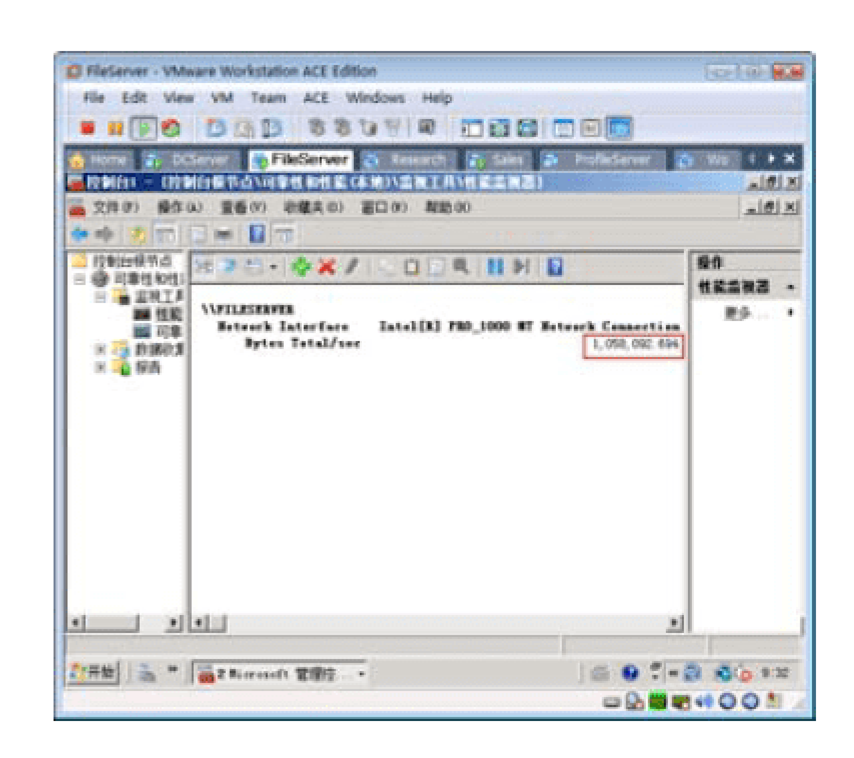


图 14-41　监控流量

第 15 章　故障转移群集

一个群集就是一组协同工作以提高服务质量和应用程序可用性的独立计算机。多台群集服务器(称为节点)之间由物理电缆和软件连接。如果其中一个节点出现故障，另外一个节点就会通过称为故障转移的一个进程开始提供服务。

在 Windows Server 2008 中，对故障转移群集(以前称为服务器群集)进行改进的目的是为了简化群集，使它们更加安全，并增强群集稳定性。群集设置和管理更加容易。同故障转移群集与存储进行通信的方法获得改进一样，群集中的安全性和联网也得到了改进。

本章内容还包括：安装和配置虚拟存储，配置 Windows Server 2008 使用 iSCSI，配置心跳线，安装故障转移群集，确定仲裁磁盘，配置文件服务器双节点群集。

关键词

- 了解什么是高可用性以及价值
- 了解什么是故障转移群集
- Windows Server 2008 的故障转移群集新特性
- 故障转移群集对硬件的要求
- 安装和配置虚拟存储
- 配置故障转移群集
- 创建文件服务器双击热备群集

15.1 高 可 用 性

第 1 章讲到了 Windows Server 2008 的新特性，其中很重要的一个就是高可用性，也许有人会说，在 Windows Server 2003 中也有关于高可用的特性，比如群集、网络负载均衡、灾难恢复等。既然作为 Server 2008 一个重要的应用场景，高可用性的改进和变化自然也是很大的，到底会有怎样的变化呢？

首先我们要明确，什么是可用性，可用性包括可靠性、故障和恢复。一个系统的可靠性、故障发生时间间隔和故障恢复速度，共同决定了这个系统的可用性。那么我们通常如何来衡量一个系统的可用性呢？最常用的方法就是使用数字“9”，通常我们会以几个“9”来说明系统的可用性。看下面这张表：

可接受的正常工作时间(%)	每天的停机时间	每月的停机时间	每年的停机时间
95	72.00 分钟	36 小时	18.26 天
99	14.40 分钟	7 小时	3.65 天
99.9	86.40 秒钟	43 分钟	8.77 小时
99.99	8.64 秒钟	4 分钟	52.56 分钟
99.999	0.86 秒钟	26 秒钟	5.26 分钟

通过这张表，我们不难发现，要做到 3 个“9”级别的系统可用性，每年只允许我们有 8.77 个小时的停机时间。当然，可用性只能用“9”，而不可能用“8”或者“7”来衡量。一个系统的高可用性，需要很多方面共同实现，如硬件、网络、操作系统、应用层面都需要有相应的高可用解决方案。在操作系统层面上，微软的 Windows Server 已经为我们提供了很好的高可用解决方案：Cluster(群集，一种并行或分布式的系统，由全面互连的计算机集合组成，可以作为一个统一的计算机资源使用)。

在此将讨论一下高可用性方案对企业用户的价值。我们经常说，或者经常会听到某个厂商说，高可用方案能够降低 TCO(总拥有成本)，可很多企业都对这个有所质疑，本来一台服务器能完成的工作，现在需要购买额外的服务器，明明硬件成本、维护成本甚至人员成本都增加了，怎么还能降低 TCO 呢？下面的例子可以说明这个问题。2007 年 10 月底的一天，时值 2008 年奥运会门票第二阶段发售之日，当时的售票策略是先到先得。于是，在发售门票开始时，便有成千上万乃至上百万的用户蜂拥到奥运门票销售网站，霎时间网站就因为并发连接过大而无法响应了。之后的一天时间中，服务器也未能恢复正常工作，以至于后来不得不改变门票的分配方式。我想对这件事情大家可能有所了解，也许是售票系统的软件设计问题，也许是硬件性能的问题，总之这套售票系统既不可靠，还发生了故障，而且未能恢复，可用性的三大方面一项也没满足，自然谈不上高可用啦。那么我们想一想没有高可用带来的损失吧，奥运是全世界瞩目的大事，在如此之大的事情上出现了这么重大的失误，造成的损失很难用金钱来衡量了。如果当初高可用方案做得很好，当然也就没有损失了，甚至可能带来很高的信誉。由此可见，高可用性方案不只会给企业增加成本，而是真正的降低了企业面临的风险，降低了 TCO。

15.2 故障转移群集概述

一个群集就是一组协同工作以提高服务质量和应用程序可用性的独立计算机。多台群集服务器(称为节点)之间由物理电缆和软件连接。如果其中一个节点出现故障，另外一个节点就会通过称为故障转移的一个进程开始提供服务。

可以使用 Microsoft 管理控制台 (MMC) 管理单元“故障转移群集管理”来验证故障转移群集配置，创建和管理故障转移群集，并将某些设置从一个运行 Windows Server 2003 的群集迁移到一个运行 Windows Server 2008 操作系统的群集。

在 Windows Server 2008 中，对故障转移群集(以前称为服务器群集)进行改进的目的是为了简化群集，使它们更加安全，并增强群集稳定性。群集设置和管理更加容易。同故障转移群集与存储进行通信的方法获得改进一样，群集中的安全性和联网也得到了改进。

应注意的是，故障转移群集功能包含在 Windows Server 2008 Enterprise 和 Windows Server 2008 Datacenter 中。它没有包含在 Windows Server 2008 Standard 或 Windows Web Server 2008 中。

Windows Server 2008 中群集的变化，首先，最明显、最直观的就是名称的变化。群集在 Windows NT4 时代就已经有了，那时叫做 Microsoft Cluster Services(MSCS)；到了 Windows 2000 时代，叫做 Server Clustering；而在 Windows Server 2008 中，群集有了个更为形象的名称，Failover Clustering(WSFC)，这个名字起的很形象，Fail——服务器故障了，Over——转移到其他机器上，正好叫做 Failover。当然，名称的改进是不会对企业用户有很大实际意义的，关键是它在技术上的改进。

15.3　Windows Server 2008 故障转移群集的新特性

15.3.1　新的确认向导功能

为了充分实现高可用性所带来的好处，必须谨慎进行全部的配置，包括服务器、网络和存储在内。Windows Server 2008 所具备的新的故障转移群集安装与配置确认向导，使用户能够对系统、存储及网络的配置是否适于集成进行确认。新的确认向导所进行的部分测试包括以下内容。

- 节点测试。确认服务器是否正在运行同样的操作系统版本及是否进行了相同的软件更新。
- 网络测试。确定是否计划的群集网络符合具体的需求，如针对网络冗余是否具有至少两个独立的子网。
- 存储测试。分析是否进行了正确的存储配置，以使所有共享的磁盘能通过全部的群集节点进行读取以及确认存储是否符合特定的需求。

15.3.2　大卷数据提高的可扩展性

Windows Server 2008 包含对全球唯一标识符(GUID)或 GUID 分区表(GPT)以集群方式存储的支持。与主引导记录(MBR)磁盘不同，GPT 磁盘能够具有大于 2000 GB 的分区以及内置的冗余。GPT 所具备的优点要大于 MBR，这是因为它允许每个磁盘进行最多 128 个的分区，并支持 18 EB 的数据量，允许对冗余进行初始和备份分区，并支持唯一的磁盘与分区标识。

15.3.3　服务器管理控制台

为简化群集的管理，群集管理界面经过改进能够让管理员集中于应用与数据的管理；而非群集的管理。新的界面基于任务设置并且更加直观，其中的向导能够帮助管理员完成之前复杂的操作。Windows Server 2008 新的故障管理群集能够使以下管理与操作任务得到简化。

- 改进的群集设置与迁移：简化了的群集设置向导使用户能够一次性完成群集的设置，同时也实现了群集的脚本可编写性，使配置流程自动化。现有群集的迁移流程也得到了简化。资源组的设置可以从运行 Windows Server 2003 的群集当中进行并应用在运行了 Windows Server 2008 的群集中。
- 简化的管理界面：在改进了向导和界面之后，管理任务得到了简化，并使管理员能够集中对应用进行管理，而不需要关注它们的群集。
- 改进的界面：用户界面基于任务设置，其中的向导能够帮助管理员完成之前复杂的操作，使现在的设置群集角色，如设置打印设备服务器角色等任务，只需几个简单的步骤便可完成。新的群集管理工具能够用于查看所有的群集角色，使配置选项成为直观的、基于任务的菜单设置。
- 快速将群集资源添加到配置：改进的群集管理界面也使共享文件夹具有高可用性等类似的任务更加容易执行。

解决群集问题 Windows 的事件跟踪功能取代了群集日志，使管理员能够通过它来轻松地搜集、管理并报告发生在群集上的事件。

- 使用卷映射复制服务来获得备份：与卷映射复制服务完全集成使备份及恢复群集的配置更加简单。
- 管理群集中共享文件夹的查看　系统提供了共享存储的查看，同时也提供了对共享文件夹的查看，这使用户能够更加轻易地了解哪些文件夹是群集，并可以进行向另一个节点的故障转移，并了解哪些共享文件夹属于本地的单一节点而不能进行故障转移。

此外，Windows Server 2008 还支持针对故障转移群集的命令行及 Windows 管理工具(WMI)选项。

15.3.4　提高的稳定性

提高了的稳定性与安全性，使可用性提高。群集与存储互动的方式获得了改进，因此仲裁资源不再成为单点故障。

Windows Server 2008 所具备的故障转移群集功能，使群集架构获得了改进并提高了向用户提供的服务质量。一个最显著的改变便是系统维护“仲裁”的方式。仲裁是确定哪些节点是活动节点，哪些节点是备用节点的群集配置数据库。它用于在节点中断时，使一个单独的节点提供所需的应用与服务。如果群集节点之间失去了互联，则会启用问题回复协议来避免裂脑(split brain)的发生。在失去互联时，节点的资源拥有者就会成为群集以及所有资源的唯一拥有者，避免了 split brain 的发生。然后这个唯一的拥有者会将所有的资源为客户可用。在拥有仲裁的节点发生故障时，现存的节点会对谁控制设备进行裁决。

故障转移群集的改进使管理员能够通过之前的 Windows 版本所具备的两种群集模式进行群集的配置。

- 仲裁磁盘模式：一个单独的磁盘作为决定允许哪部分集群继续运行的“投票者”。
- 占多数节点设置模型：只有在占多数的节点是在运行良好状态及互联时才会使群集继续运行。

在 Windows Server 2008 上，这两种模式的混合操作作为默认的配置，使两种模式的优势都能够得到发挥。例如，在双节点的群集中，即使仲裁磁盘出现故障而完全不可用时群集也能够继续运行。管理员无须处理复杂的仲裁配置，这些都在设置群集的过程中得到了自动配置。在这种新的混合模式下，每个节点都有复制的仲裁资源，因此仲裁磁盘出现的故障不会导致群集出现故障。

15.3.5　存储集成

Windows Server 2008 故障转移群集在存储集成方面的改进使功能与可靠性与之前的服务器群集版本相比有了很大的提高。主要表现在：动态添加磁盘资源；资源在线时可对资源的相关性进行修改。

- 数据存储的性能与稳定性得到了提高：Windows Server 2008 采用了持久保留功能及新的管理共享文件方式而获得了改进。它不再使用可能造成 SAN 中断的 SCSI 总线重设。Windows Server 2008 的故障转移群集使磁盘不再处于不受保护的状态，意味着卷受到破坏的可能性减小了。故障转移群集还改进了对磁盘的查找和恢复，并支持 3 种类型的存储连接：序列连接 SCSI(Serial Attached SCSI)，SAS 以及光纤通道。
- 更轻松的磁盘维护：维护模式得到了许多改进，管理员可以更加轻松地运行工具来检查、修复、备份或恢复磁盘，同时降低对群集造成的影响。

15.3.6　网络连接与安全性

由于改进了网络连接和安全性能，网络运行状况与安全性能通过集成 IPv6，使用不依赖旧有的 NetBIOS(网络基本输入/输出系统)的 DNS(域名系统)服务器而获得了改进，同时其他的网络连接方面的改进也使企业网络更加稳定，配置更加安全。

Windows Server 2008 的故障转移群集使网络连接与安全性能与之前的版本相比获得了提高，具体表现在以下几个方面。

- 使用完全与故障转移群集集成的 IPv6：故障转移群集完全支持 IPv6 进行节点到节点以及节点到客户端的通信。
- 使用域名系统(DNS)而不再依靠旧有的 NetBIOS：简化了服务器信息块的转移，并意味着用户不再需要 Windows 互联网名称服务(WINS)以及 NetBIOS 名称解析。
- 通过对网络连接的其他改进使可靠性提高：管理员能够使网络名称资源与多个相关的 IP 地址具备关联性，使 IP 地址可用时，网络名称也可用。除此之外，在节点传输并接收“频率”来确认每个节点仍然可用时，使用更加可靠的传输控制协议(TCP)，而不是可靠性较低的用户数据图表协议(UDP)。

故障转移群集对安全性能的改进包括以下方面。

- 新的安全模式：Windows Server 2008 保护改进的安全模式，其中群集服务运行在 LocalSystem 内置账号的环境下，使安全性和对账号密码的保护得到增强。
- 审核：管理员可以通过使用审核来捕捉关于读取群集的用户信息以及读取时间信息。
- 加密：Windows Server 2008 运行管理员将内部节点互连设为加密。
- 不同 IP 子网上的节点：群集中的节点不再需要位于同一个 IP 子网，因而提高了灵活性。当集群在地理位置上延伸而地点变得灵活时这个改进尤为重要。

总结

Windows Server 2008 中的故障转移群集为需要传输关键应用与服务的企业提供了简单易用的解决方案。新的配置特征使高可用性的故障转移集群能够更加容易生成与配置，新的管理界面则通过统一的管理故障转移群集接口减少了操作的复杂性与费用。

15.4 配置 Windows Server 2008 群集

1. 实验目的

- 了解 Windows Server 2008 故障转移群集的架构。
- 能够使用 Windows Server 2008 连接 iSCSI 网络存储。
- 配置 Windows Server 2008 群集。
- 能够在 Windows Server 2008 群集中安装 SQL Server 2008。

2. 实验环境

图 15-1 所示为实际企业环境中 Windows Server 2008 群集的网络连接，群集中的两个节点通过单独的光纤交换机连接到网络存储设备。“心跳网络”为群集之间的专用网络。

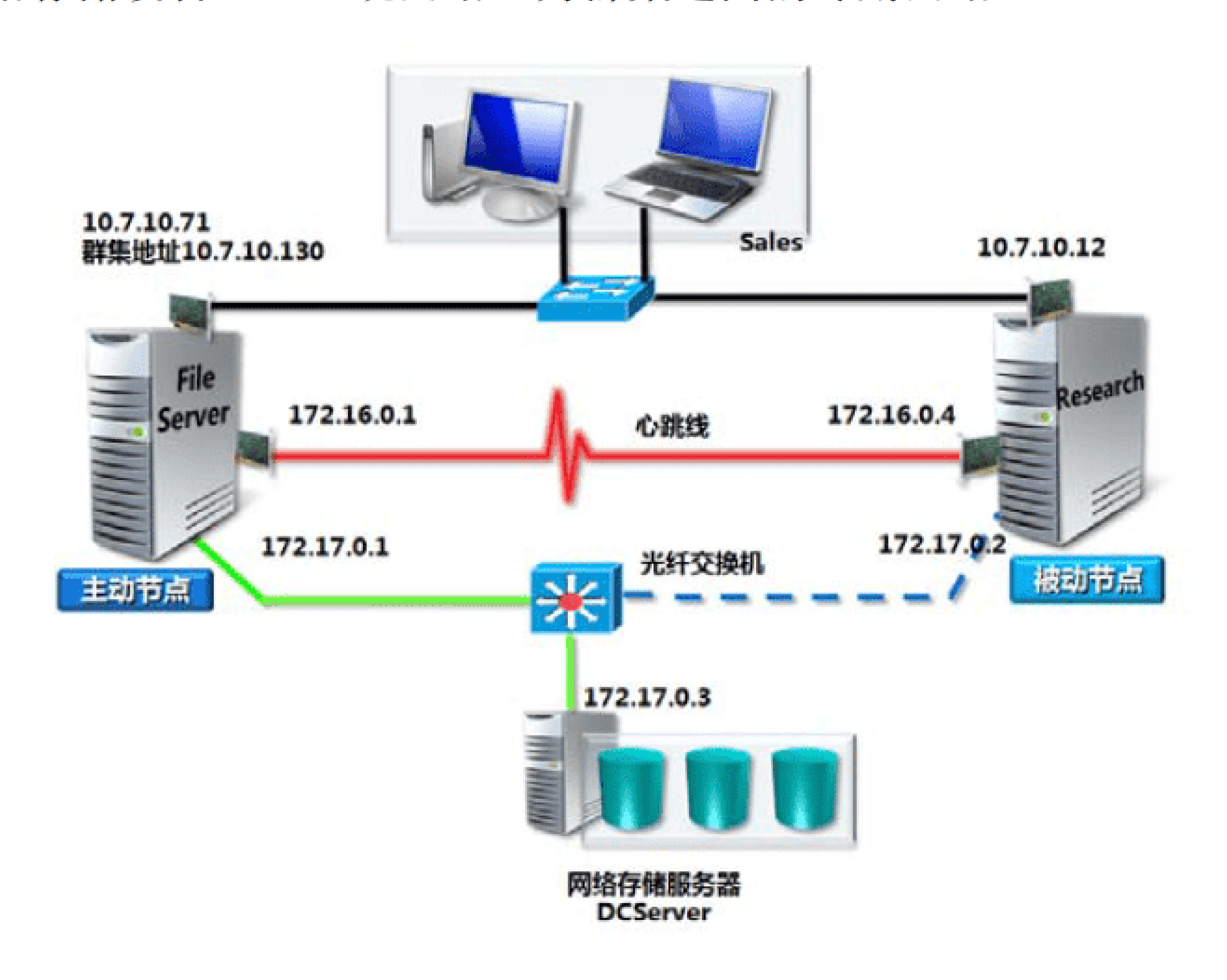


图 15-1 企业环境群集环境

如图 15-2 所示为本章实验的环境，群集中的两个节点将不使用专门的交换机和网络存储服务器连接。

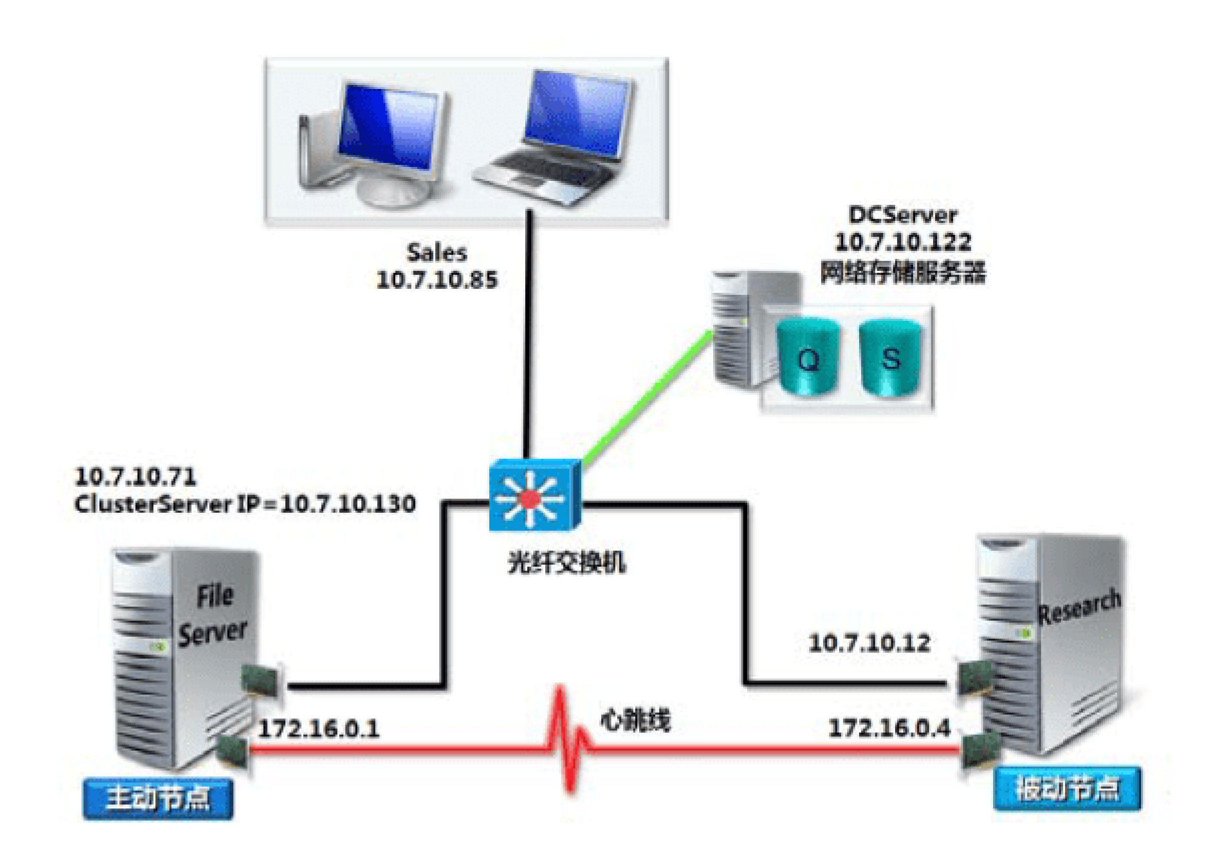


图 15-2 实验群集环境

DCServer 安装 Windows Server 2008 企业版，是 Ess.com 域的域控制器。

FileServer 和 Research 服务器安装 32 位 Windows Server 2008 企业版，是 Ess.com 域的成员，将会配置作为群集中的两个节点。

Sales 安装的 Vista 操作系统，是 Ess.com 域中的计算机。

3. IP 地址配置

群集系统包括两套网络，一套是对外提供网络服务的网络，本例中名称为“网络测试”的网络；一套是群集节点服务器之间交互的网络，本例中名称为“心跳网络”的网络。心跳网络 IP 地址设置时，仅设置 IP 地址和子网掩码即可，DNS 参数和默认网关不需要设置。在“高级 TCP/IP 设置”对话框中，选中“禁用 TCP/IP 上的 NETBIOS” 选项。其他需要注意的问题如下。

每个节点服务器上均拥有静态 IP 地址，服务器群集不支持使用由动态主机配置协议服务器分配的地址。

每个节点服务器至少必须拥有两个网络适配器，一个用于连接客户端的“网络测试”网络，另一个用于连接节点服务器对节点服务器专用群集“心跳网络”网络。

所有节点服务器都必须拥有两个面向公用和专用通信的物理独立的局域网或虚拟局域网。

DCServer 域控制器配置参数如下。

- IP 地址：10.7.10.122。
- 子网掩码：255.255.255.0。
- Active Directory 名称：Ess.com。
- DNS 服务器：10.7.10.122。
- 计算机名称：DCServer。

节点 FileServer 服务器配置参数如下。

- IP 地址：10.7.10.71。
- 子网掩码：255.255.255.0。
- 连接心跳线网卡 IP 地址：172.16.0.1。
- 子网掩码：255.255.0.0。
- Active Directory 名称：Ess.com。
- DNS 服务器：10.7.10.122。
- 计算机名称：FileServer。

节点 Research 服务器配置参数如下。

- IP 地址：10.7.10.12。
- 子网掩码：255.255.255.0。
- 连接心跳线网卡 IP 地址：172.16.0.4。
- 子网掩码：255.255.0.0。
- Active Directory 名称：Ess.com。
- DNS 服务器：10.7.10.122。
- 计算机名称：Research。

群集节点服务器配置参数如下。

- IP 地址：10.7.10.130。
- 子网掩码：255.255.255.0。
- 计算机名称：ClusterServer。

15.5 安装和配置虚拟存储

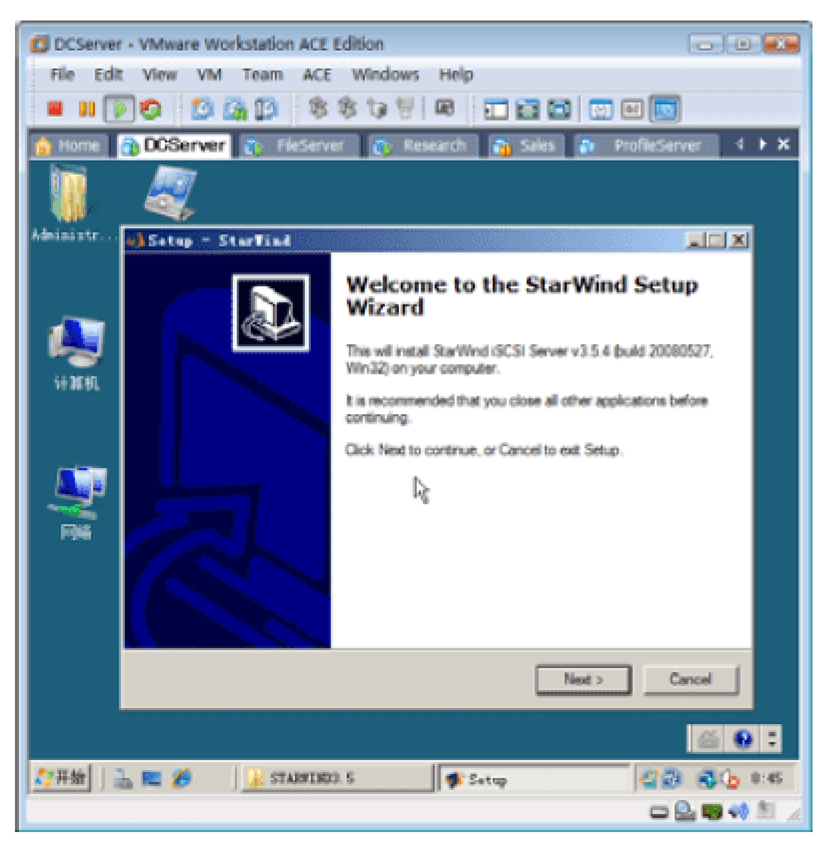
存储服务器是部署群集的基础，大多数用户没有专门的存储服务器。下面以虚拟存储为例，介绍搭建存储服务器的方法。

15.5.1 安装 StarWind

本例中搭建存储服务器使用 StarWind 软件，该软件可以模拟 iSCSI 存储服务。在 http://www.rocketdivision.com/网站中下载 X32 版本 StarWind 的软件。

① 如图 15-3 所示，在 DCServer 上，安装 StarWind，运行后启动安装向导，单击 Next 按钮。

② 如图 15-4 所示，在 License Agreement 界面中，选中 I access the agreement 单选按钮，单击 Next 按钮。



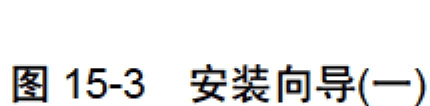


图 15-3 安装向导(一)

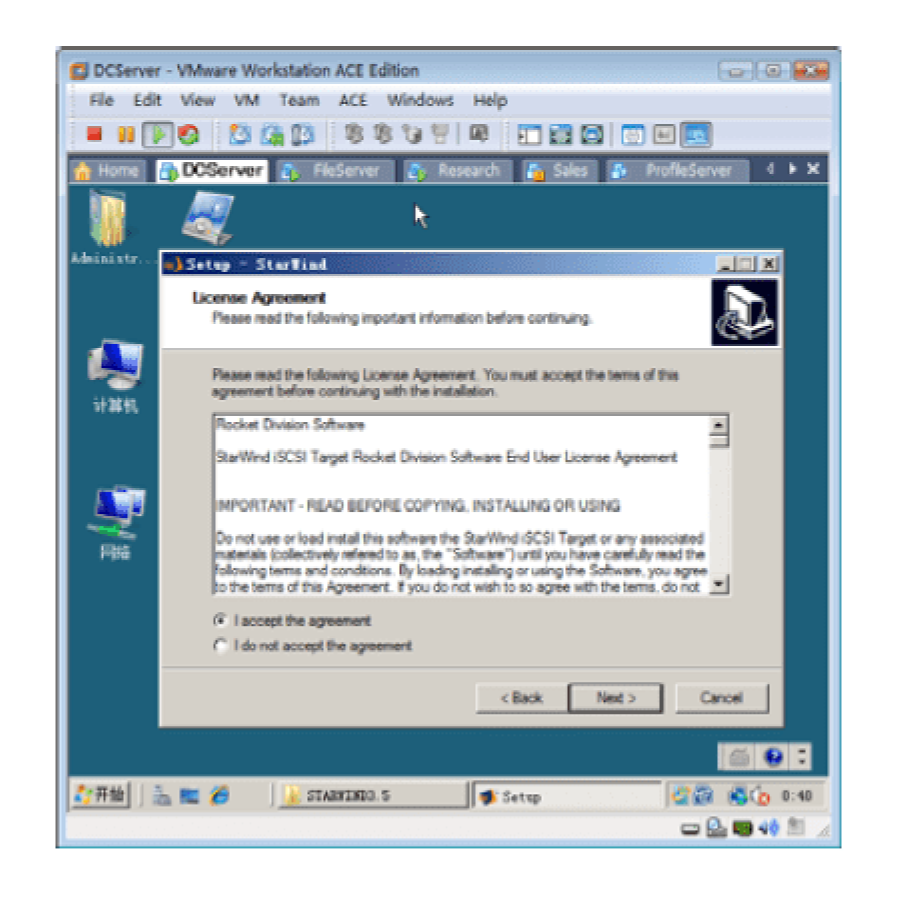


图 15-4 安装向导(二)

③ 如图 15-5 所示，在 Select Destination Location 界面中，设置 StarWind 安装的目标文件夹，使用默认值即可，单击 Next 按钮。

④ 如图 15-6 所示，在 Select Components 界面中，选择安装的组件。本例选择完整安装，单击 Next 按钮。

⑤ 如图 15-7 所示，在 Select Start Menu Folder 界面中，设置启动菜单，使用默认值默认即可。单击 Next 按钮。

⑥ 如图 15-8 所示，在 Select Additional Tasks 界面中，选中 Create a desktop icon 复选框，单击 Next 按钮。

⑦ 如图 15-9 所示，在出现的 Ready to Install 界面中，显示设置参数，单击 Install 按钮。

⑧ 如图 15-10 所示，安装完成，单击 Finish 按钮，完成 StarWind 的安装。

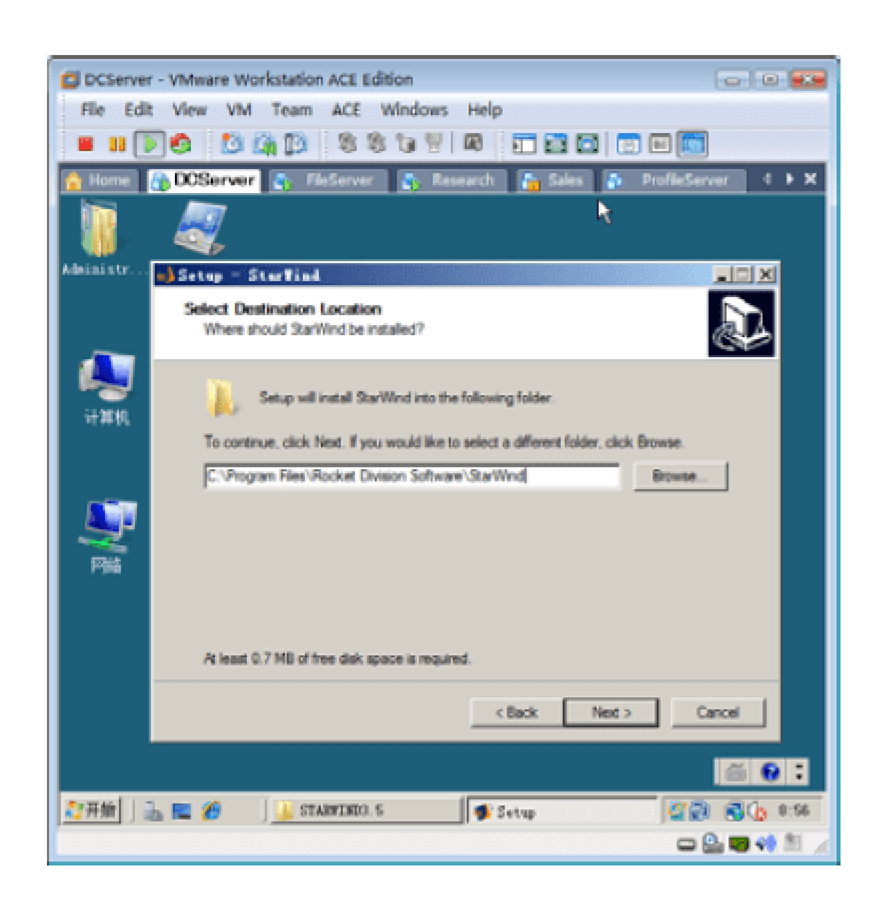


图 15-5　选择安装路径

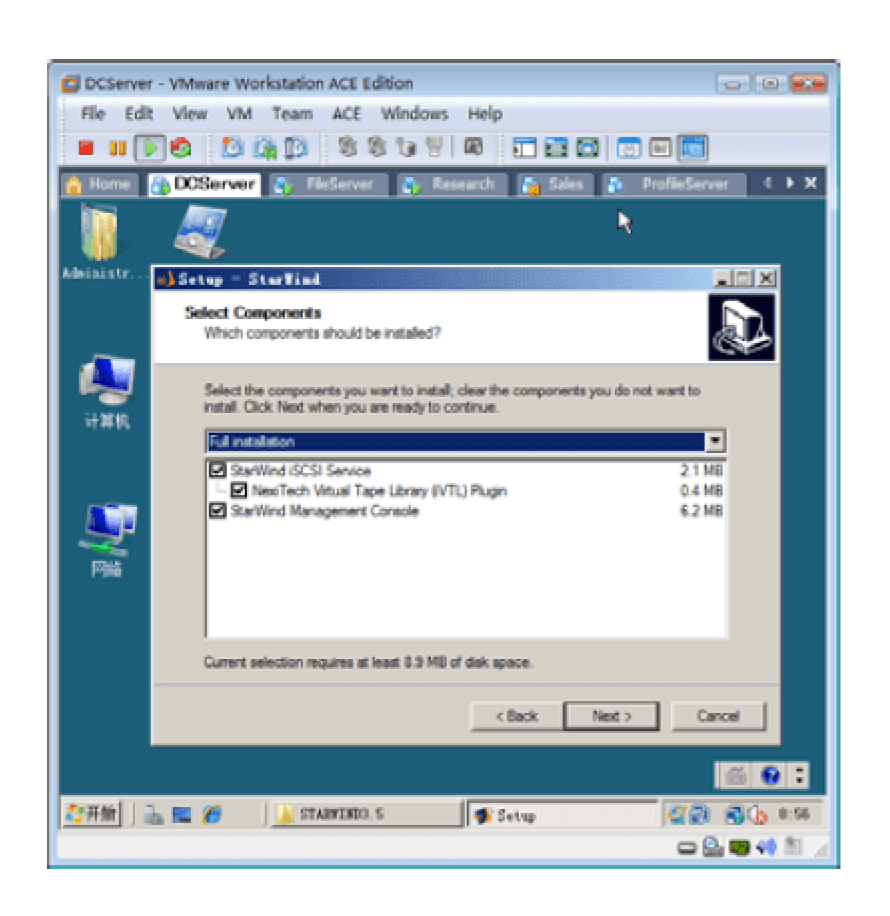


图 15-6　选择安装组件

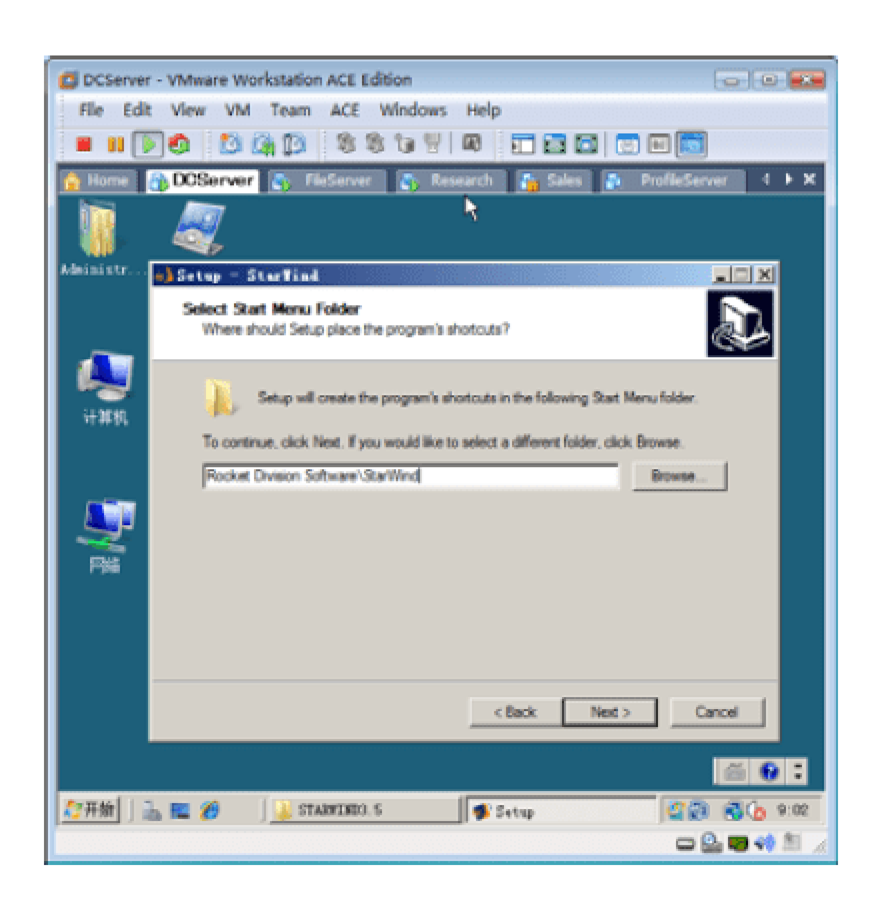


图 15-7　选择开始菜单文件夹

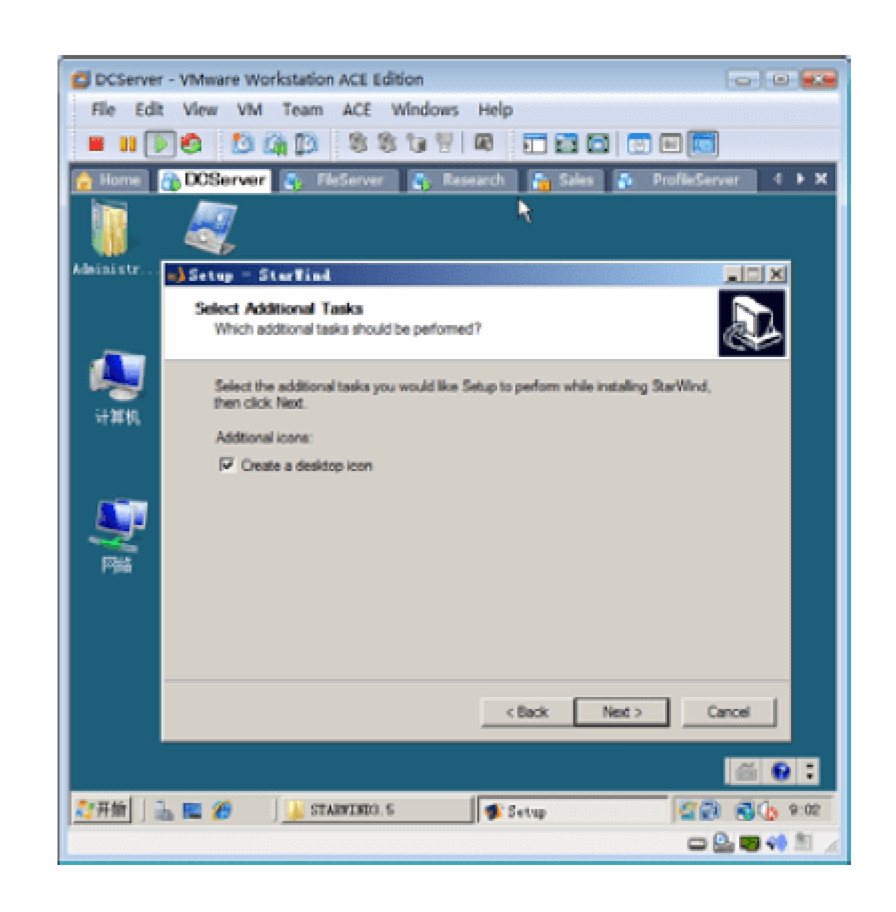


图 15-8　创建桌面图标

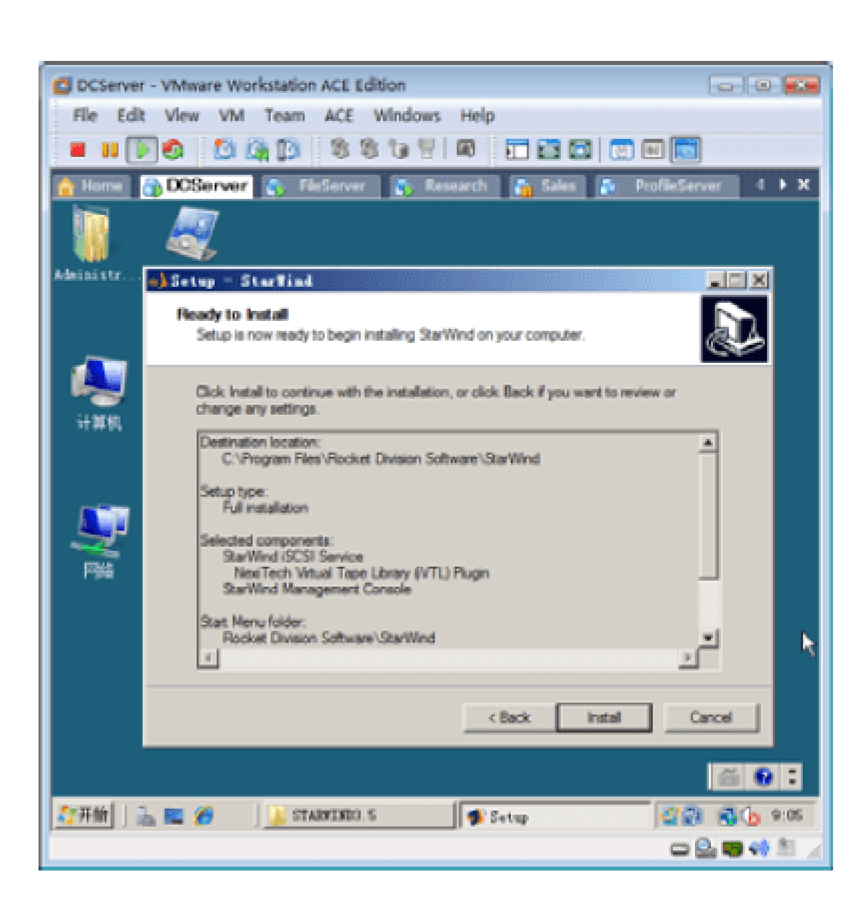


图 15-9　安装向导

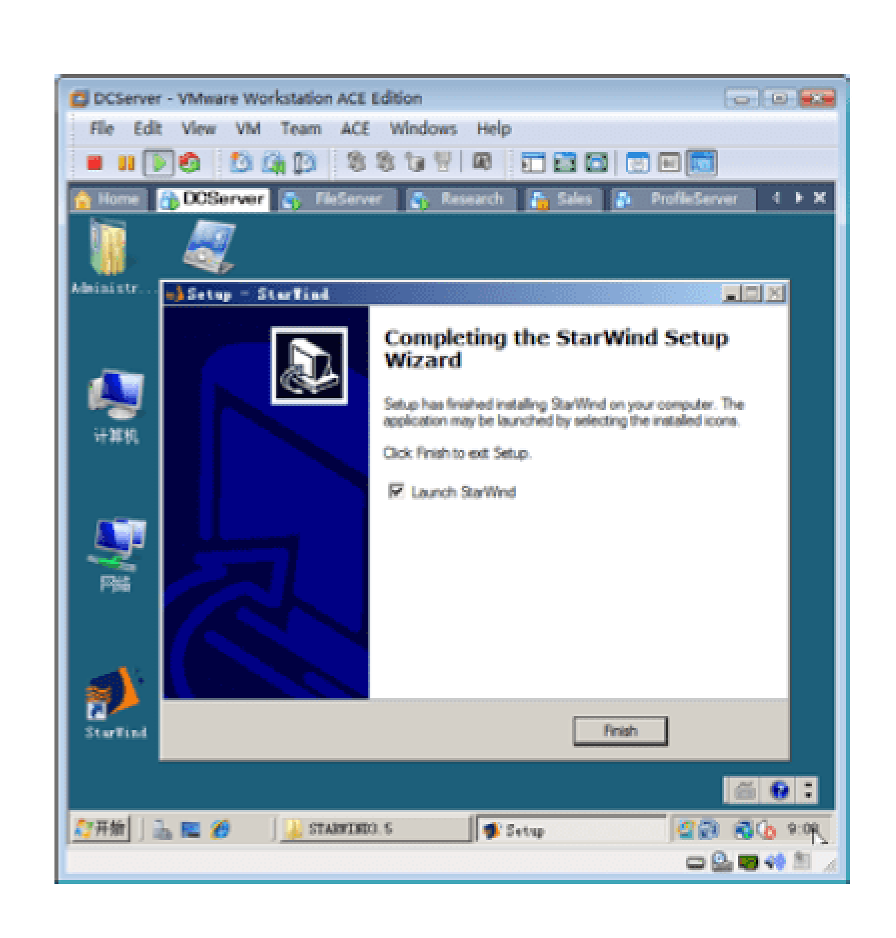


图 15-10　完成安装

15.5.2 配置 StarWind

Windows Server 2008 的故障转移群集，需要用到两块磁盘，一块磁盘为仲裁磁盘，一块磁盘为数据磁盘。下面介绍使用 StarWind 创建磁盘的方法。

① 如图 15-11 所示，选择“开始”→“所有程序”→Rocket Division Software→StarWind→StarWind 命令，或单击工具栏中的按钮，显示 StarWind 窗口。

② 如图 15-12 所示，右击“localhost:3260”，在弹出的快捷菜单中选择 Connect 命令。

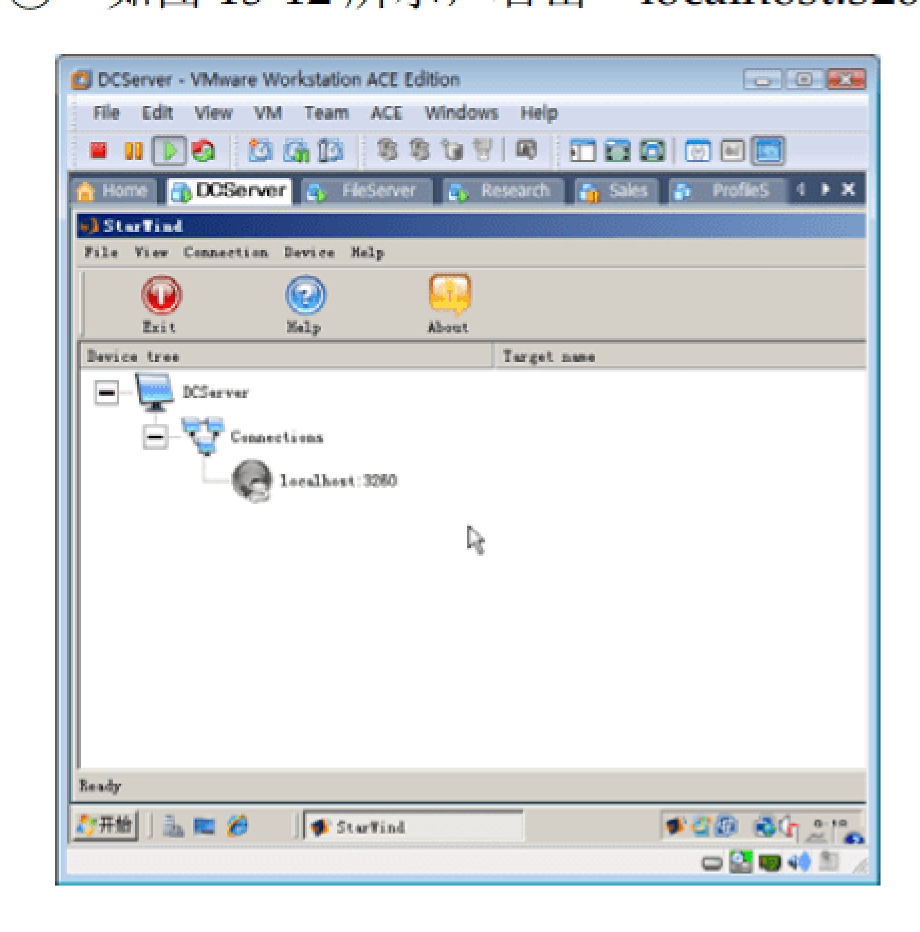


图 15-11 打开 StarWind 窗口

图 15-12 连接

③ 如图 15-13 所示，在 User name 和 Password 文本框中，输入用户名和密码，用户名和密码均为 test，单击 OK 按钮，连接成功。

④ 连接成功后，“localhost:3260”以高亮度显示，如图 15-14 所示。

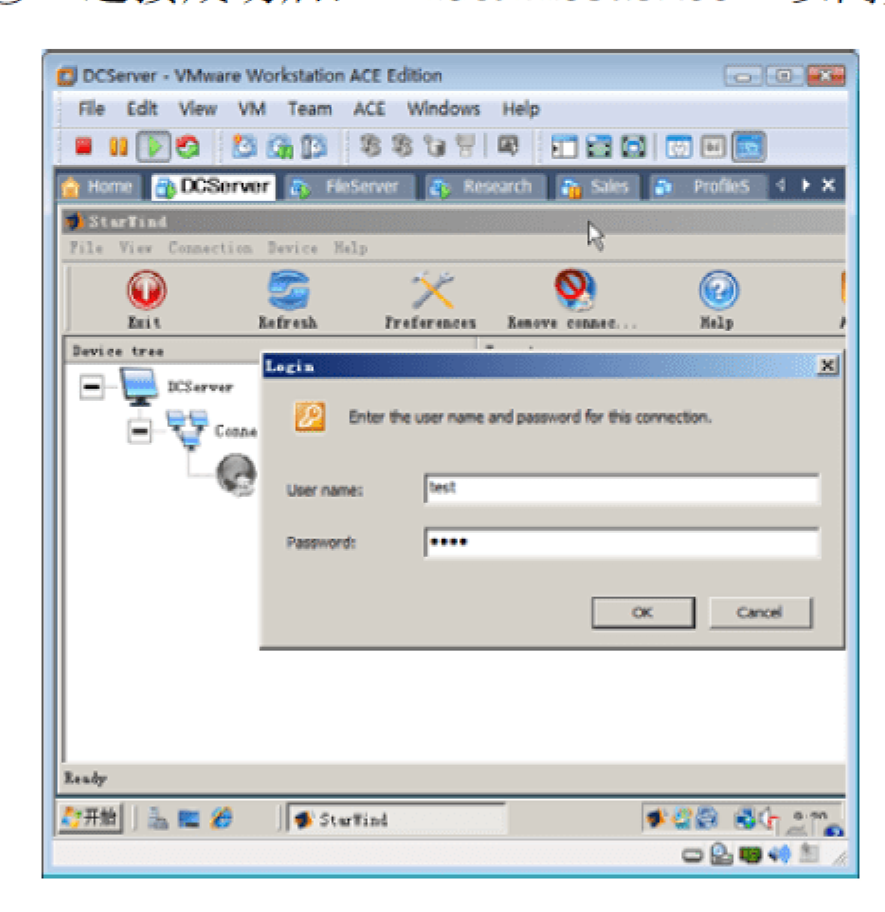


图 15-13 输入账号和密码

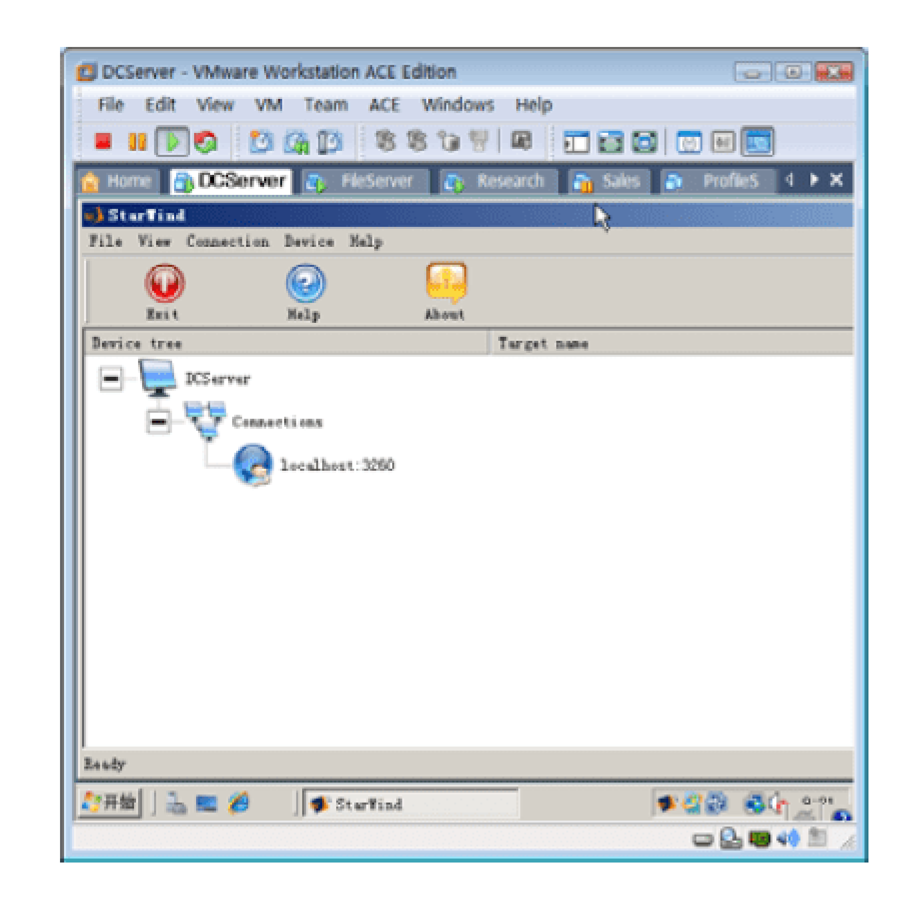
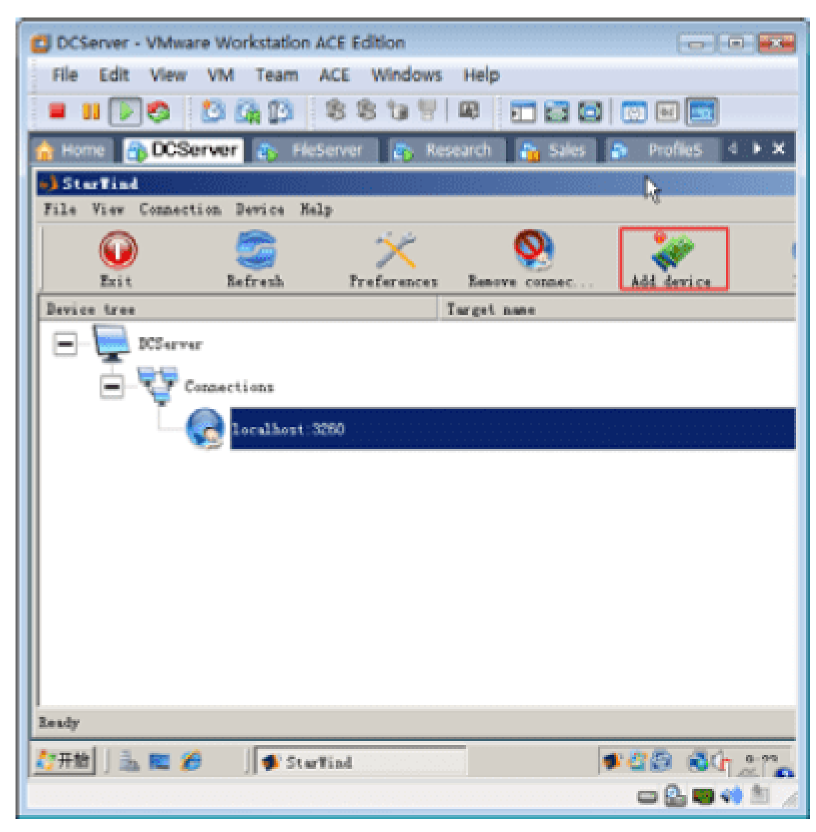


图 15-14 连接成功后

⑤ 如图 15-15 所示，选中“Localhost:3260”，单击 Add device 按钮。

⑥ 如图 15-16 所示，启动设备增加向导，在 Please Select a device type 界面中，选择增加的设备。本例中选中 Image File device 单选按钮，创建一个映像文件设备，单击“下一步”按钮。



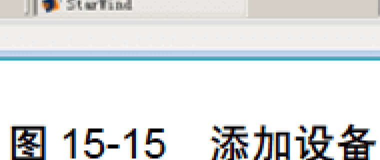


图 15-15　添加设备

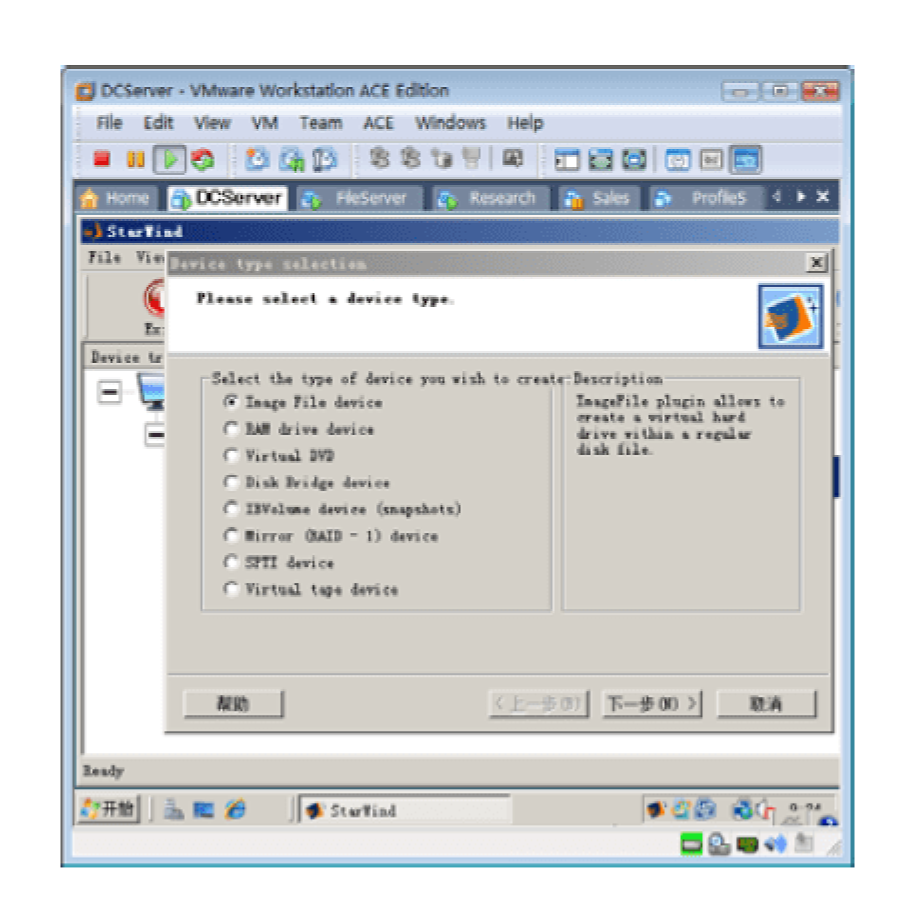


图 15-16　选择设备类型

⑦　如图 15-17 所示，在 Please select method to add selected device 界面中，提供加载现有映像文件和创建新映像文件选项。本例中选中 Create new image 单选按钮，单击“下一步”按钮。

⑧　如图 15-18 所示，在 Specify ImageFile image parameters 对话框中，单击 ... 按钮。

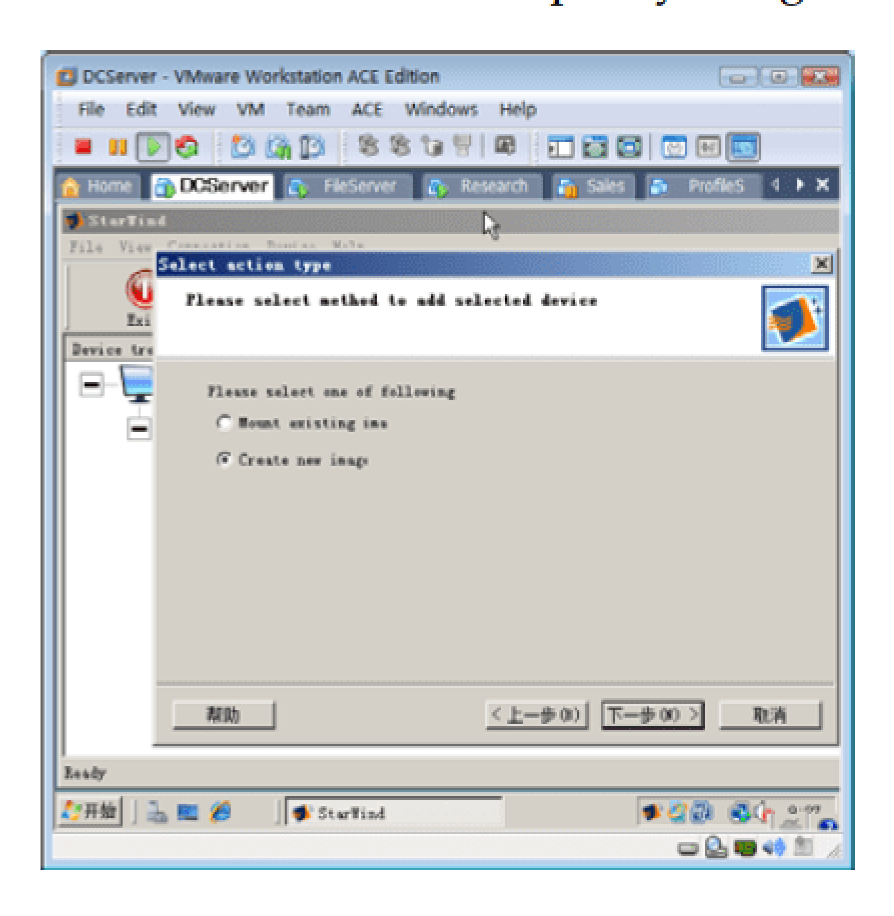


图 15-17　创建一个映像

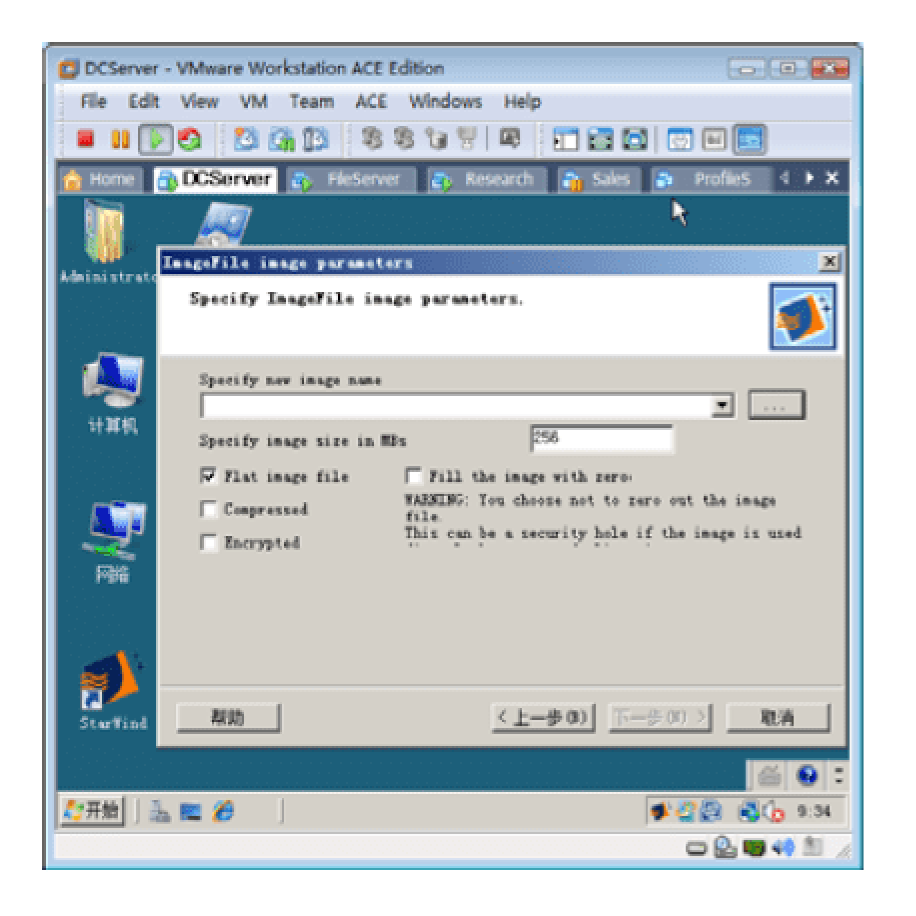


图 15-18　指定映像位置

⑨　如图 15-19 所示，在 Open image 对话框中，设置存储映像文件的目标文件夹，以及文件名称，单击 OK 按钮。

⑩　如图 15-20 所示，输入 image 的大小为 1000，单击“下一步”按钮。

⑪　如图 15-21 所示，在 Please specify Image File device parameters 界面中，选中 Allow multiple concurrent iSCSI connections(clustering)复选框，允许多人连接该设备。

⑫　如图 15-22 所示，在 Please specify common device parameters 界面中，设置设备的公用名称，单击“下一步”按钮。

⑬　如图 15-23 所示，在 Completing the Add Device Wizard 界面中，显示新设备相关的参数，单击“下一步”按钮。

⑭　如图 15-24 所示，在 Completing the Add Device Wizard 界面中，完成设备的创建。

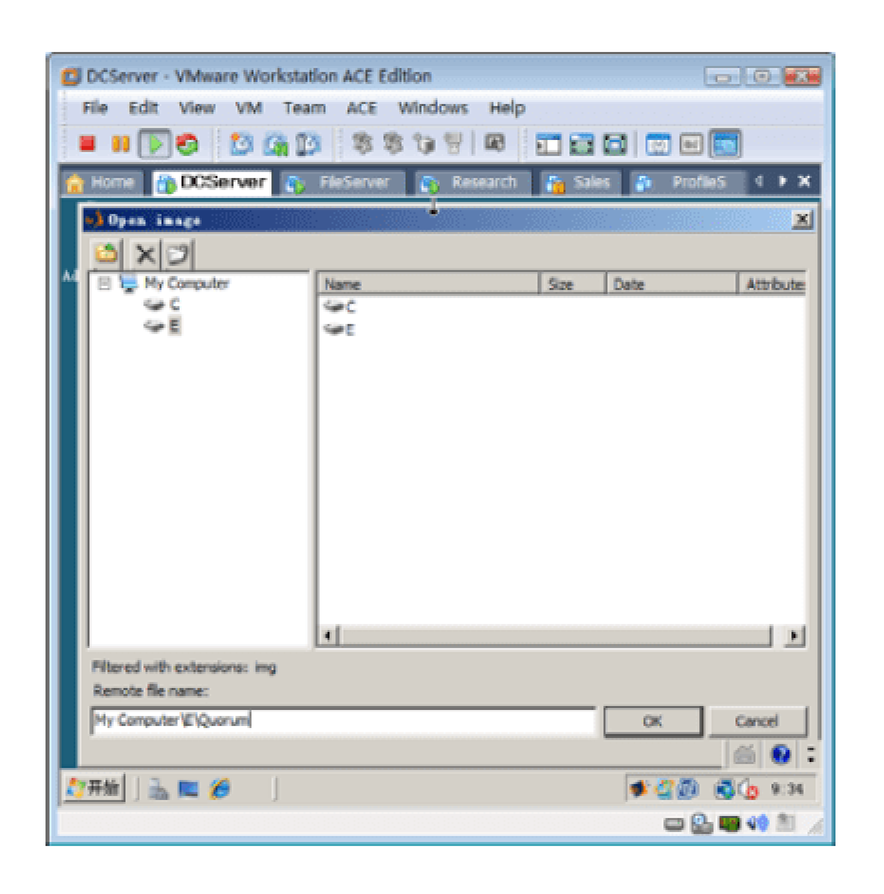


图 15-19　打开映像

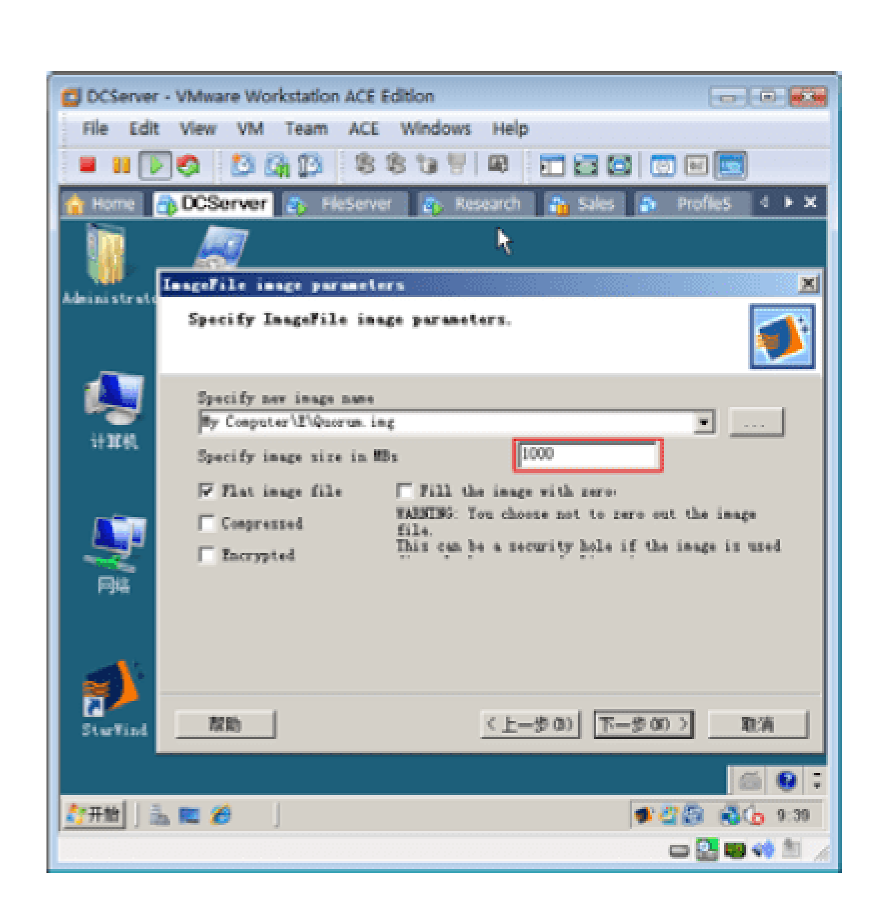


图 15-20　指定大小

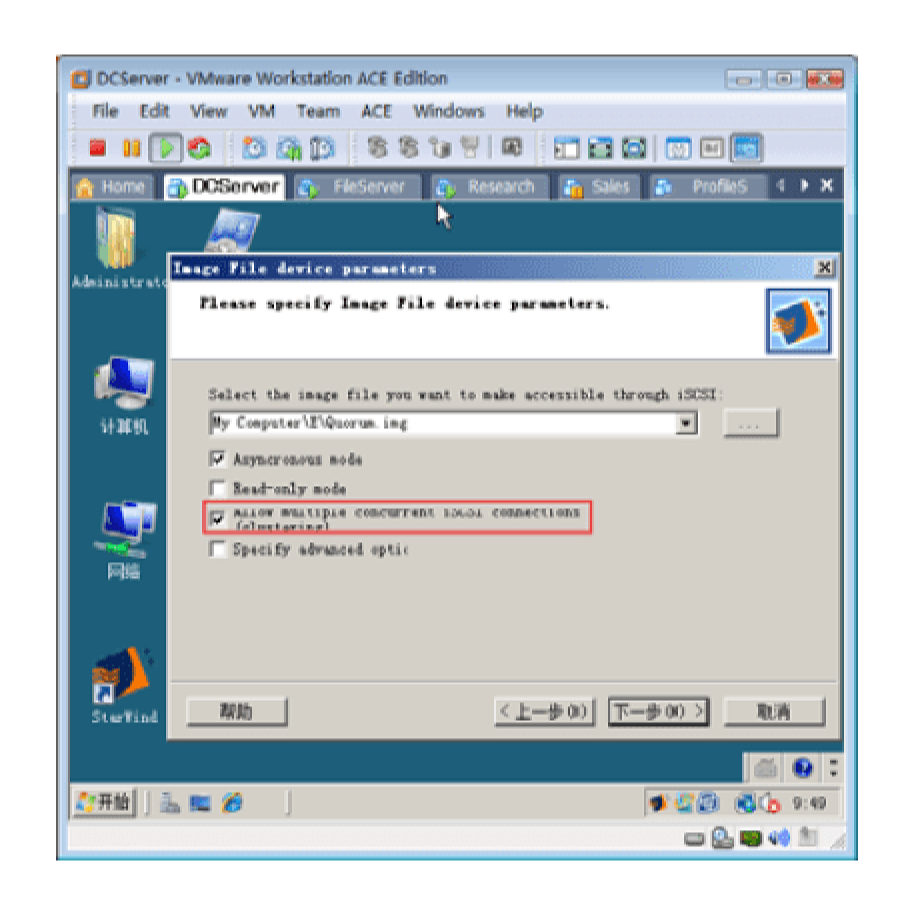


图 15-21　允许多个连接

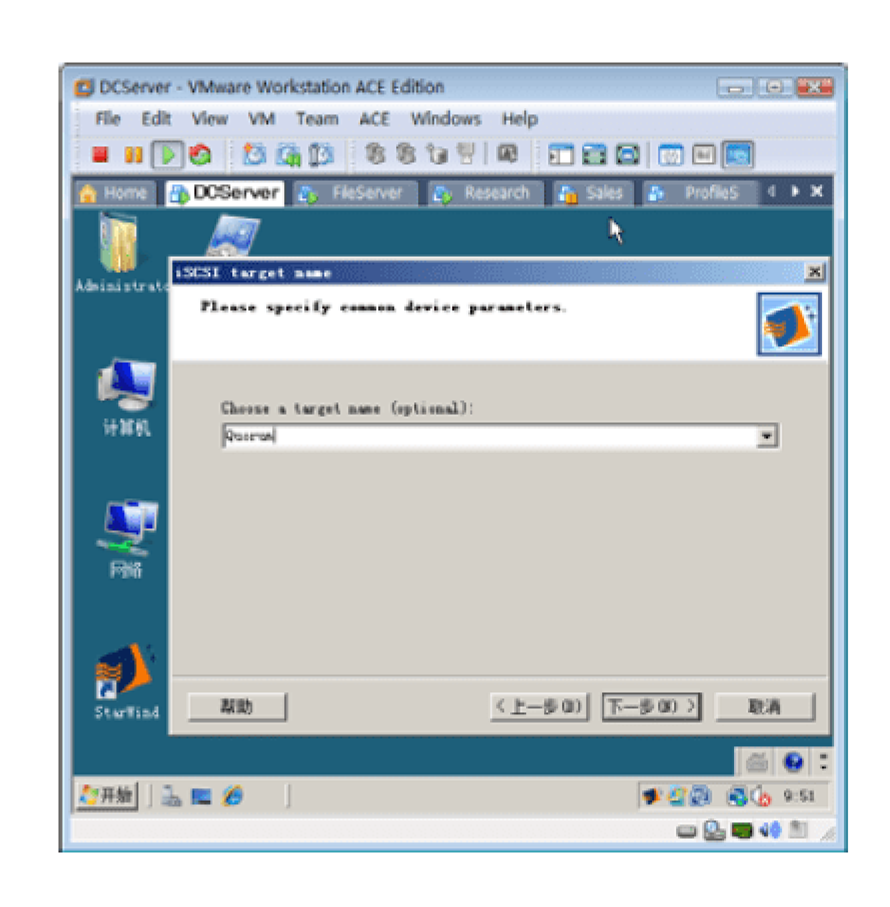


图 15-22　设置公用名称

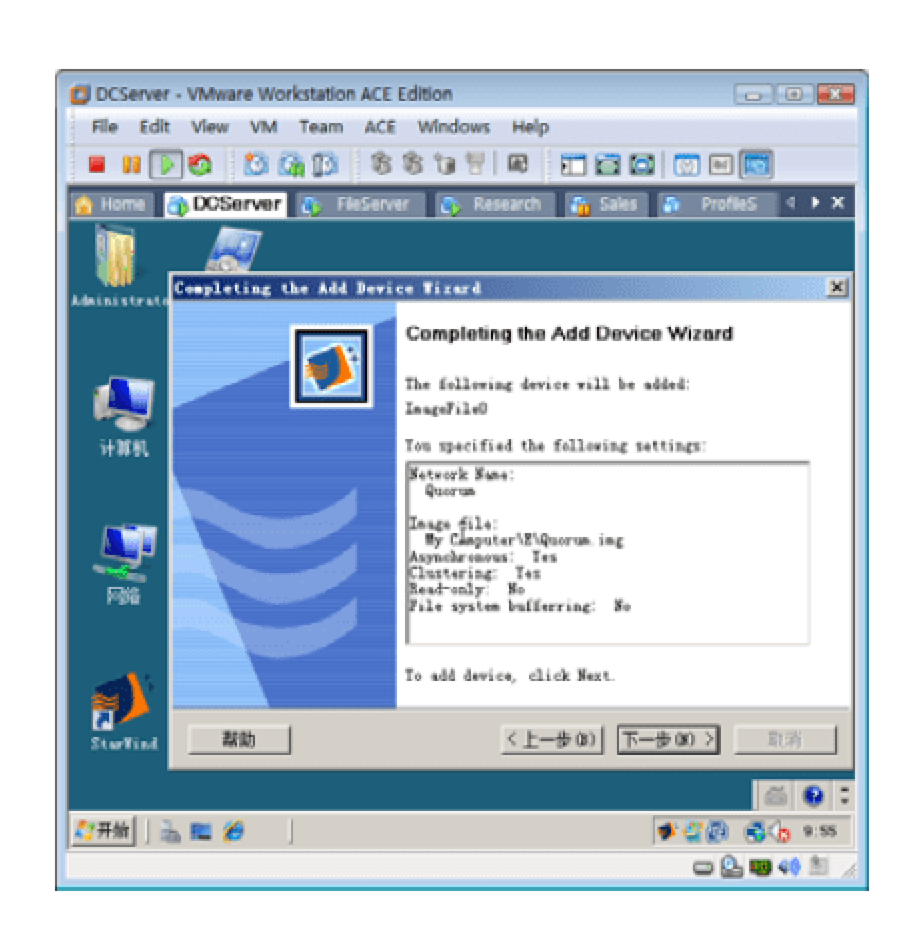


图 15-23　添加设备向导

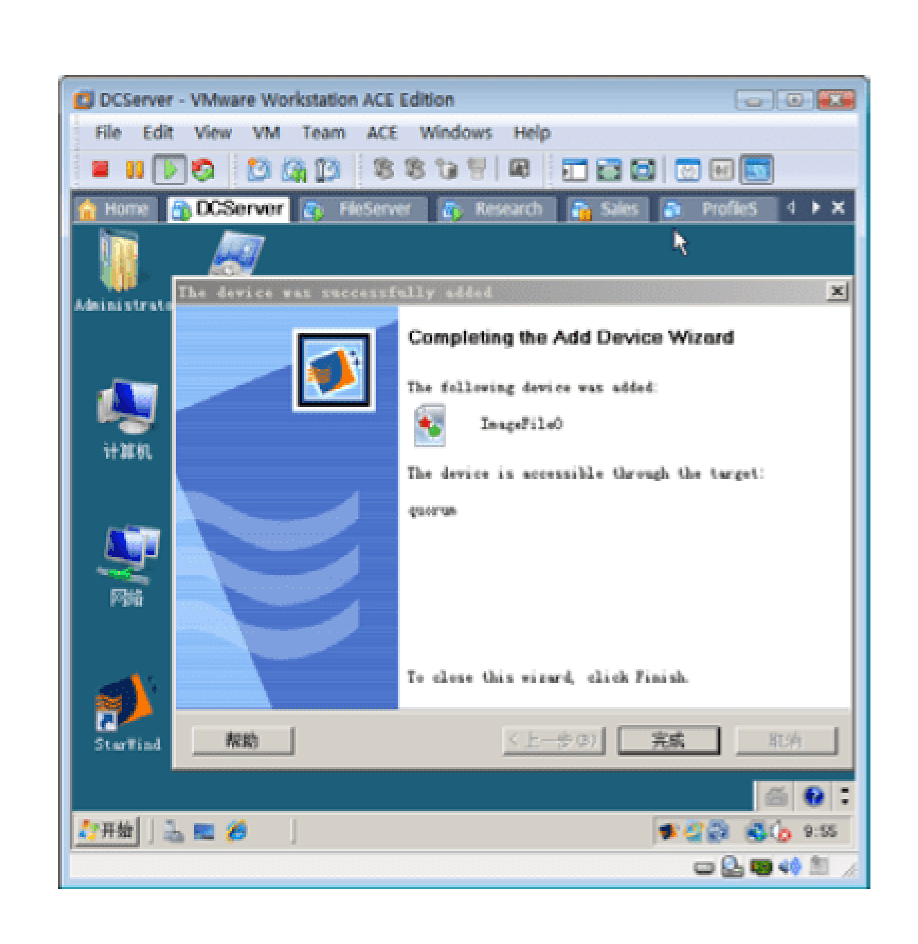


图 15-24　完成添加设备向导

⑮　如图 15-25 所示，用同样的方法创建 Data 磁盘，指定磁盘大小为 2000 MB。

⑯　创建完成的磁盘如图 15-26 所示。

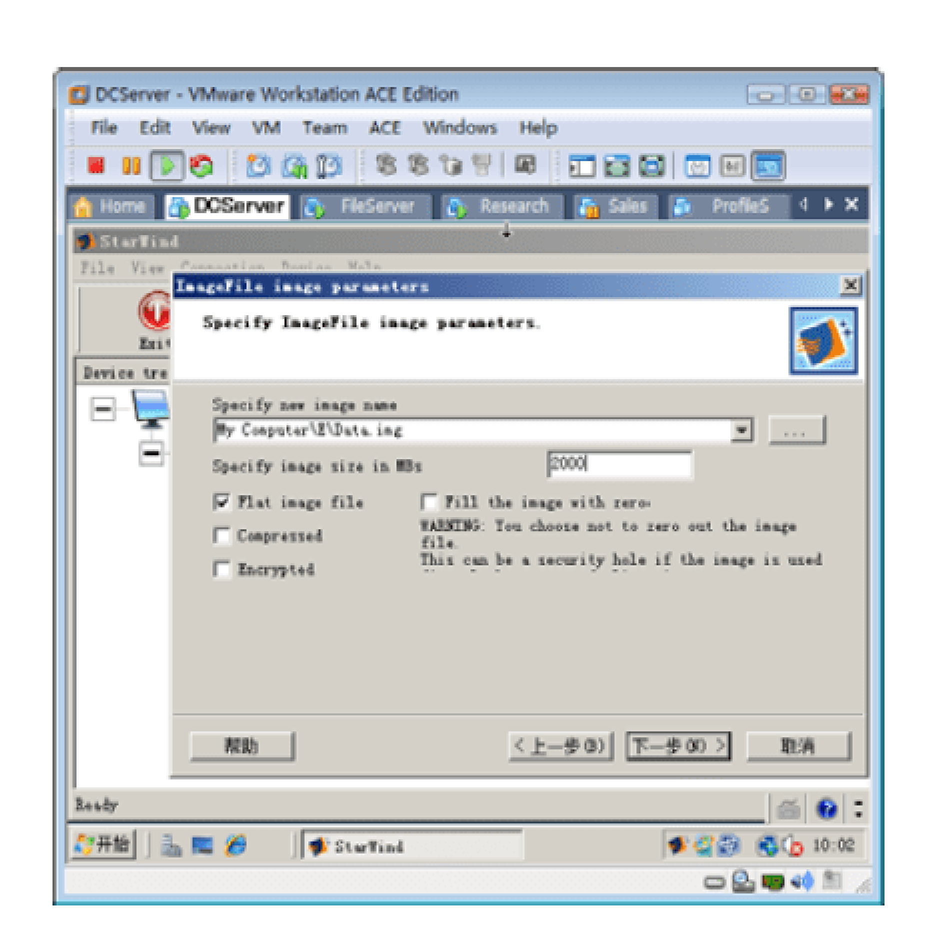


图 15-25　指定映像和大小

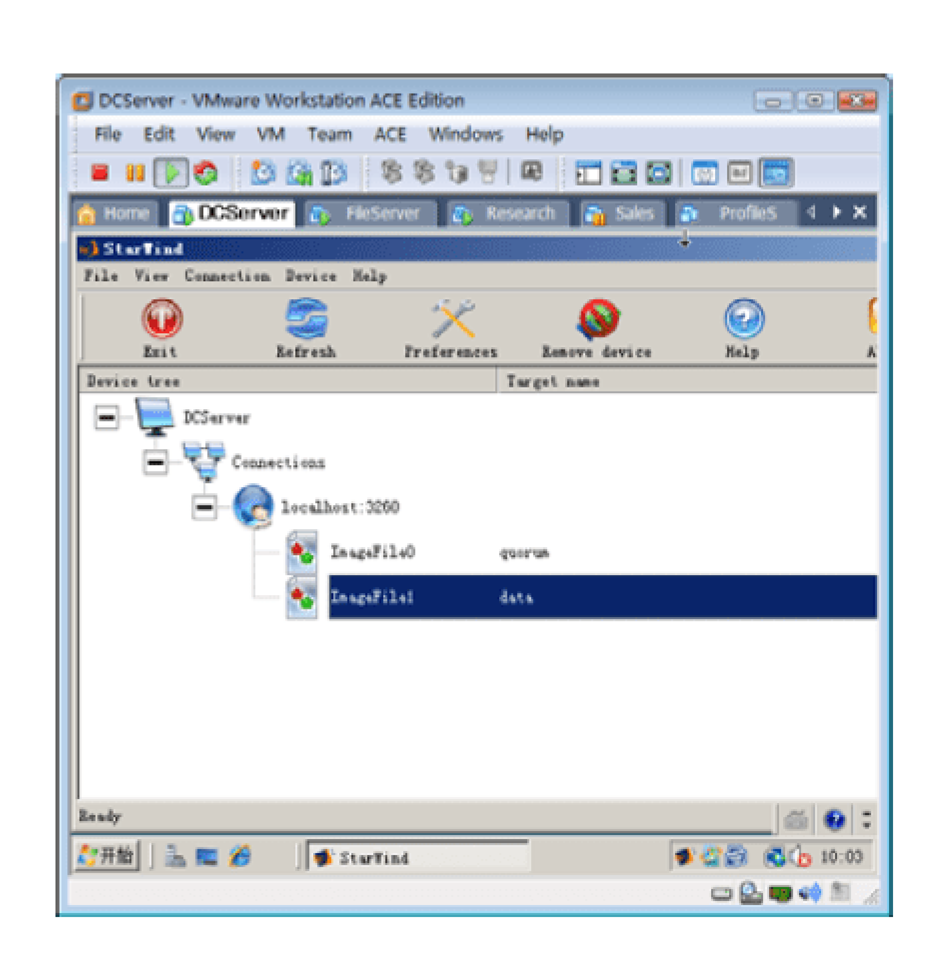


图 15-26　添加的两个磁盘

15.5.3　在节点 FileServer 配置 iSCSI

群集服务中的节点 FileServer 服务器添加存储服务之前，需要将节点 FileServer 服务器添加到 Active Directory 中，并以域网络管理员身份登录。

① 如图 15-27 所示，选择“开始”→“控制面板”命令，打开“控制面板”窗口。

② 如图 15-28 所示，双击“iSCSI 发起程序”图标，在 Microsoft iSCSI 对话框中，单击“是”按钮，启动并在以后开机时自动启动 iSCSI 服务。

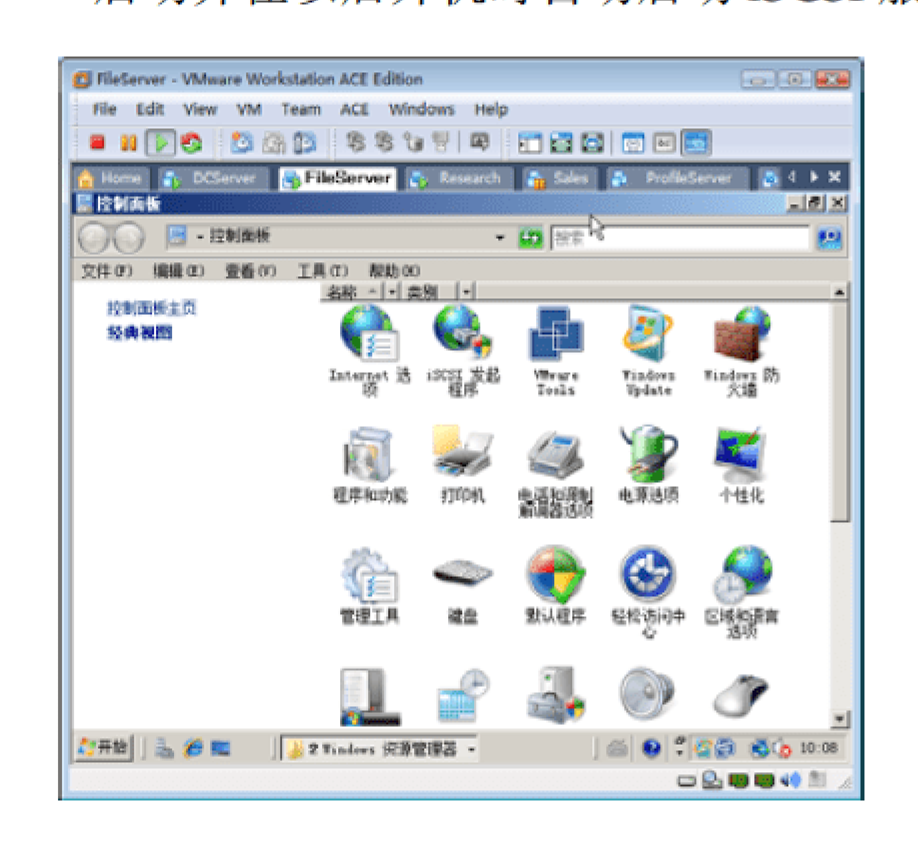


图 15-27　打开 iSCSI 发起程序

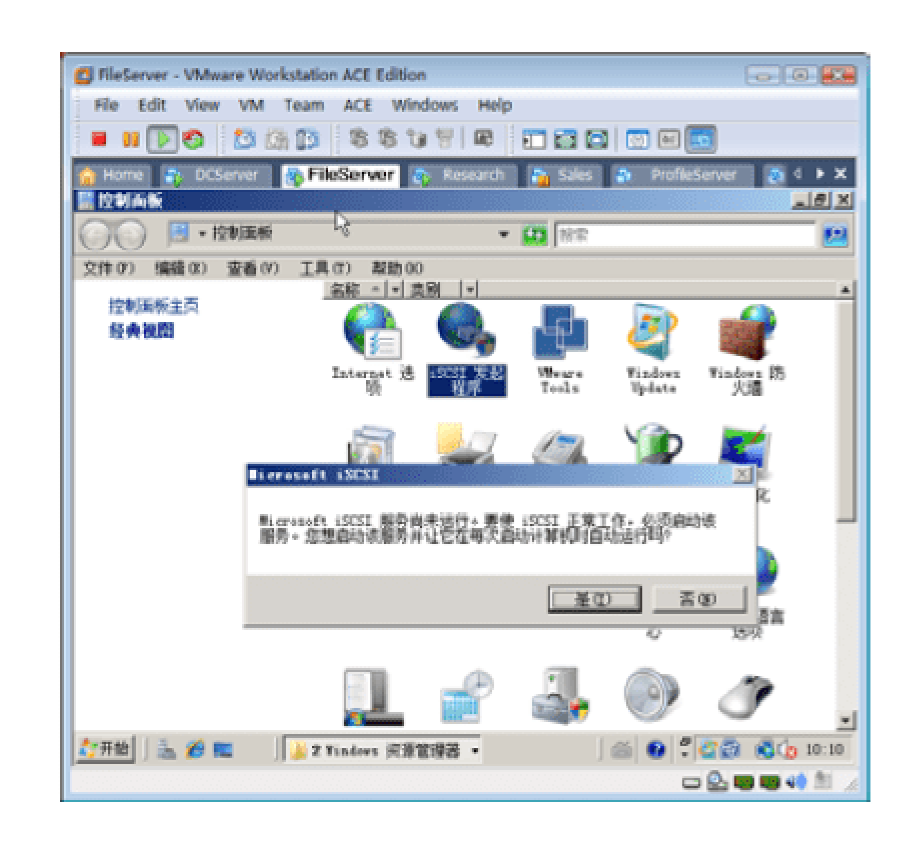


图 15-28　启动 iSCSI 服务

③ 如图 15-29 所示，在 Microsoft iSCSI 对话框中，提示将允许 iSCSI 服务穿透防火墙，单击“是”按钮。

④ 如图 15-30 所示，在“iSCSI 发起程序 属性”对话框中，切换到“发现”选项卡。

⑤ 如图 15-31 所示，单击“添加门户”按钮，在出现的“添加目标门户”对话框中，输入 10.7.10.122，单击“确定”按钮。

⑥ 如图 15-32 所示，切换到“目标”选项卡，选中 data，单击“登录”按钮，在出现的对话框中选中“计算机启动时自动还原此链接”复选框，单击“确定”按钮。



图 15-29　开启防火墙端口

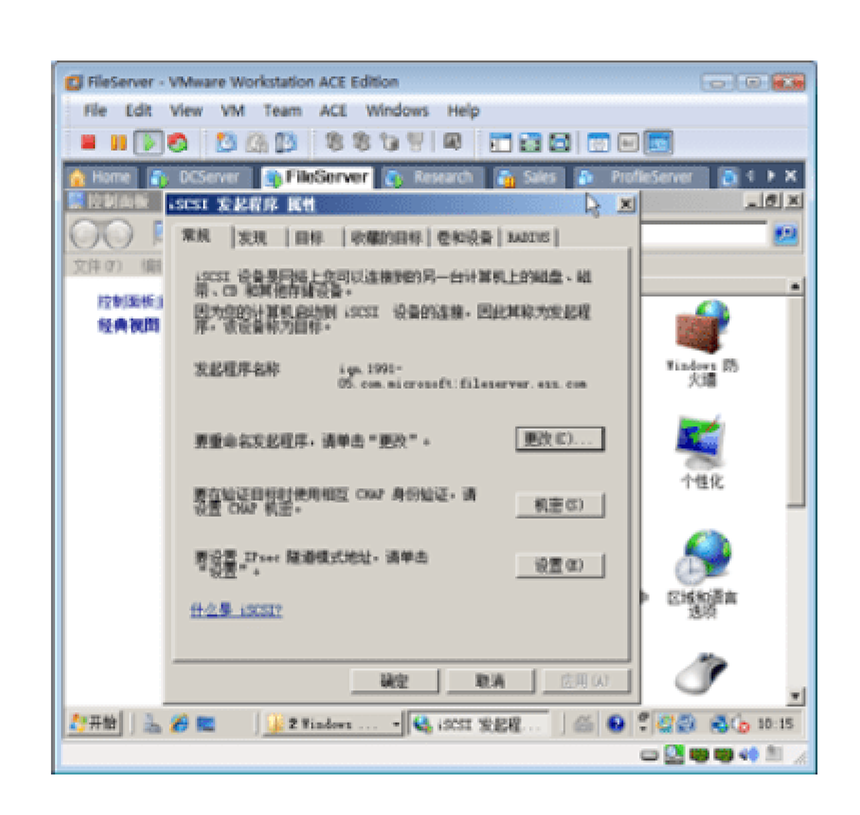


图 15-30　配置 iSCSI

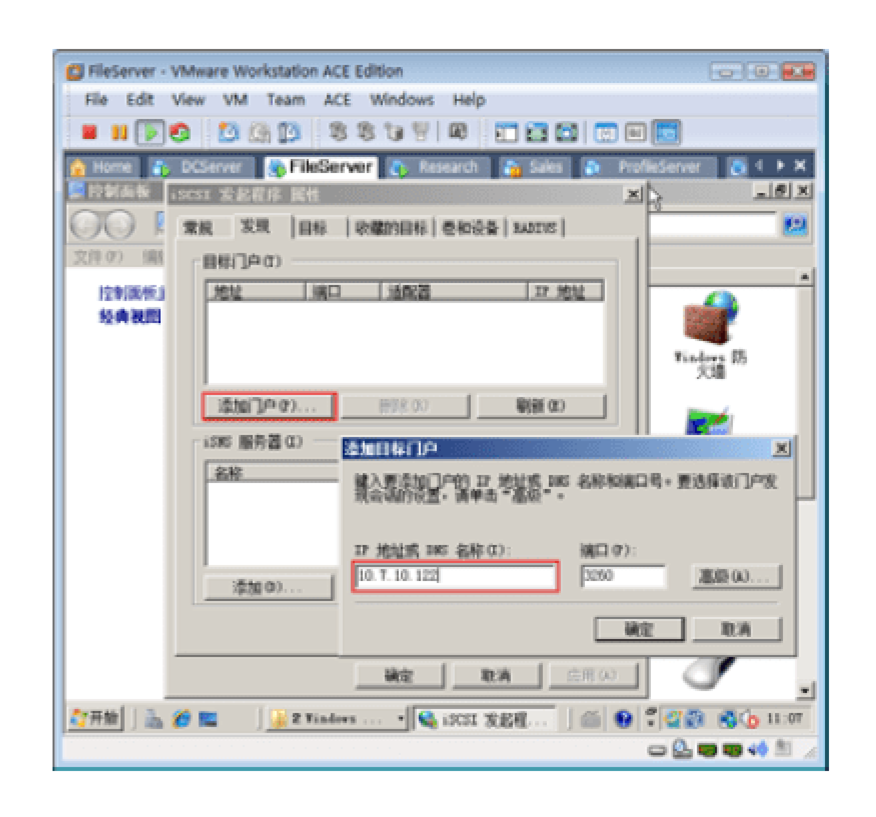


图 15-31　输入门户地址和端口

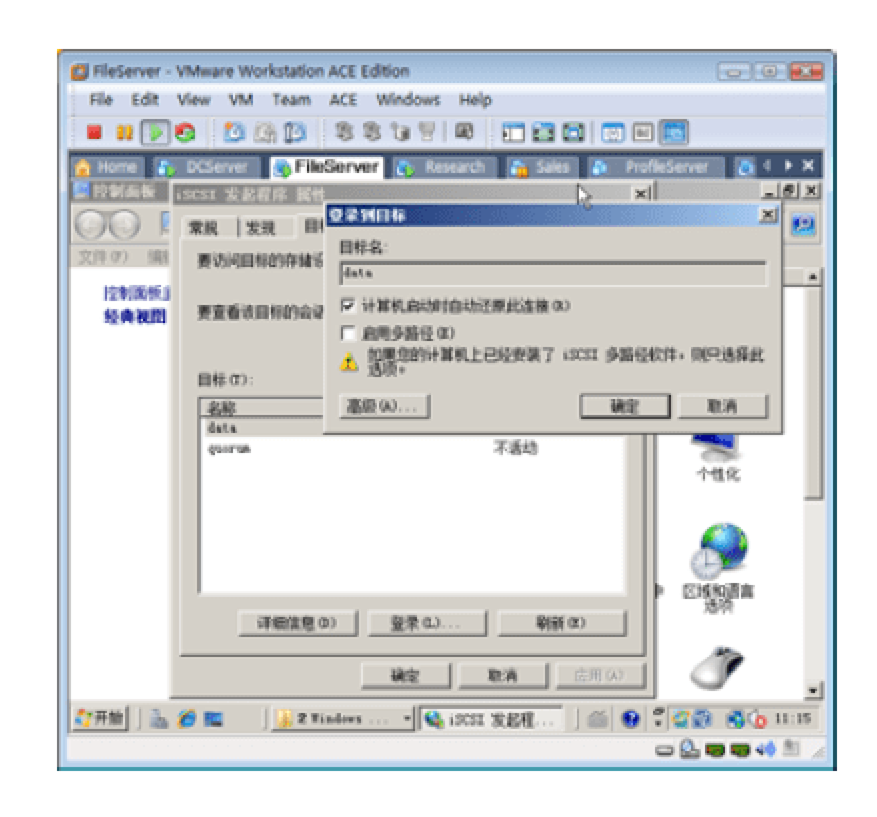


图 15-32　连接设备

⑦ 如图 15-33 所示，选中 quorum，单击“登录”按钮，在出现的对话框中选中“计算机启动时自动还原此链接”复选框，单击“确定”按钮，可以看到两个目标的状态为已连接。单击“确定”按钮，完成 iSCSI 服务的设置。

⑧ 选择“开始”→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口，如图 15-34 所示。展开“服务器管理器(FileServer)”→“存储”→“磁盘管理”节点，如图所示，已经成功添加了两块磁盘。

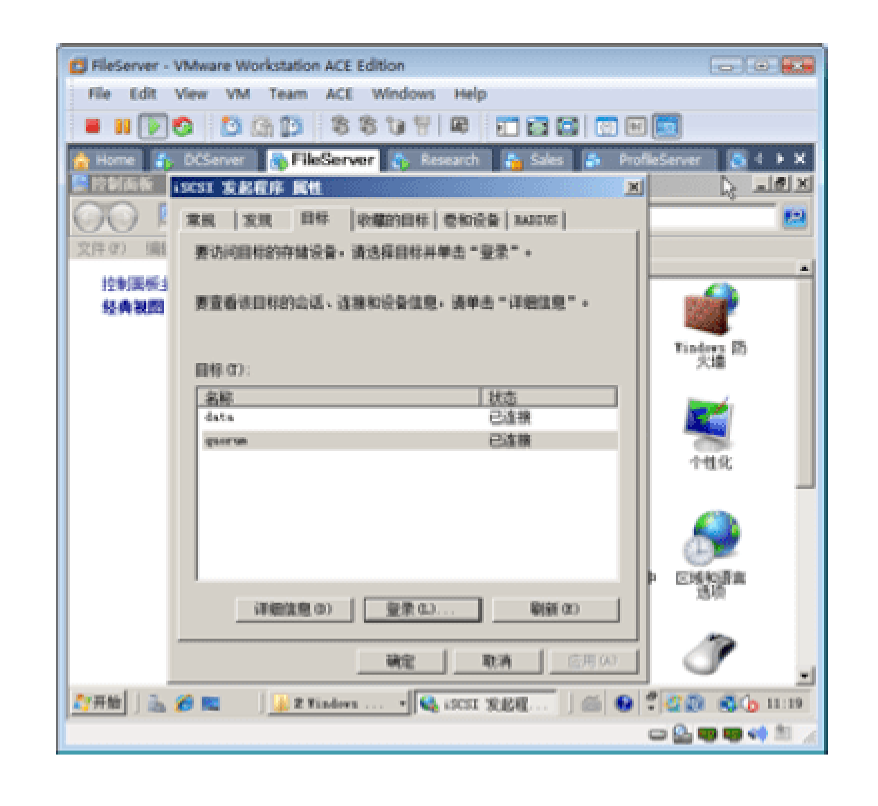


图 15-33　两个设备均连接

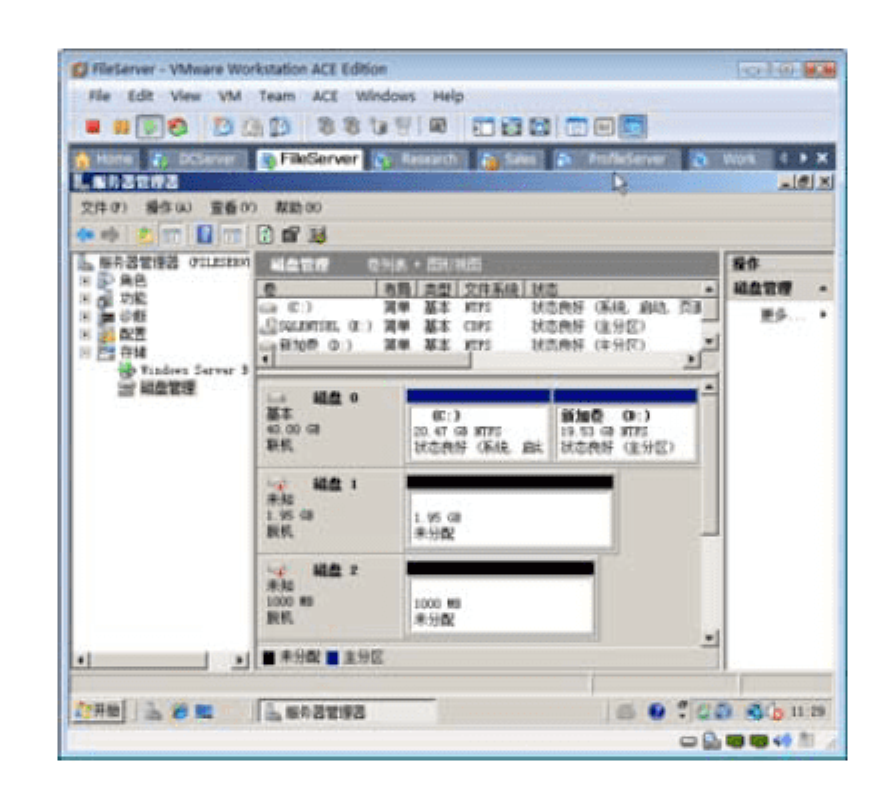


图 15-34　可以看到 iSCSI 建立的磁盘

⑨　如图 15-35 所示，右击磁盘 1，从弹出的快捷菜单中选择“联机”命令，右击磁盘 2，从弹出的快捷菜单中选择“联机”命令。

⑩　如图 15-36 所示，右击磁盘 1，从弹出的快捷菜单中选择“初始化磁盘”命令。

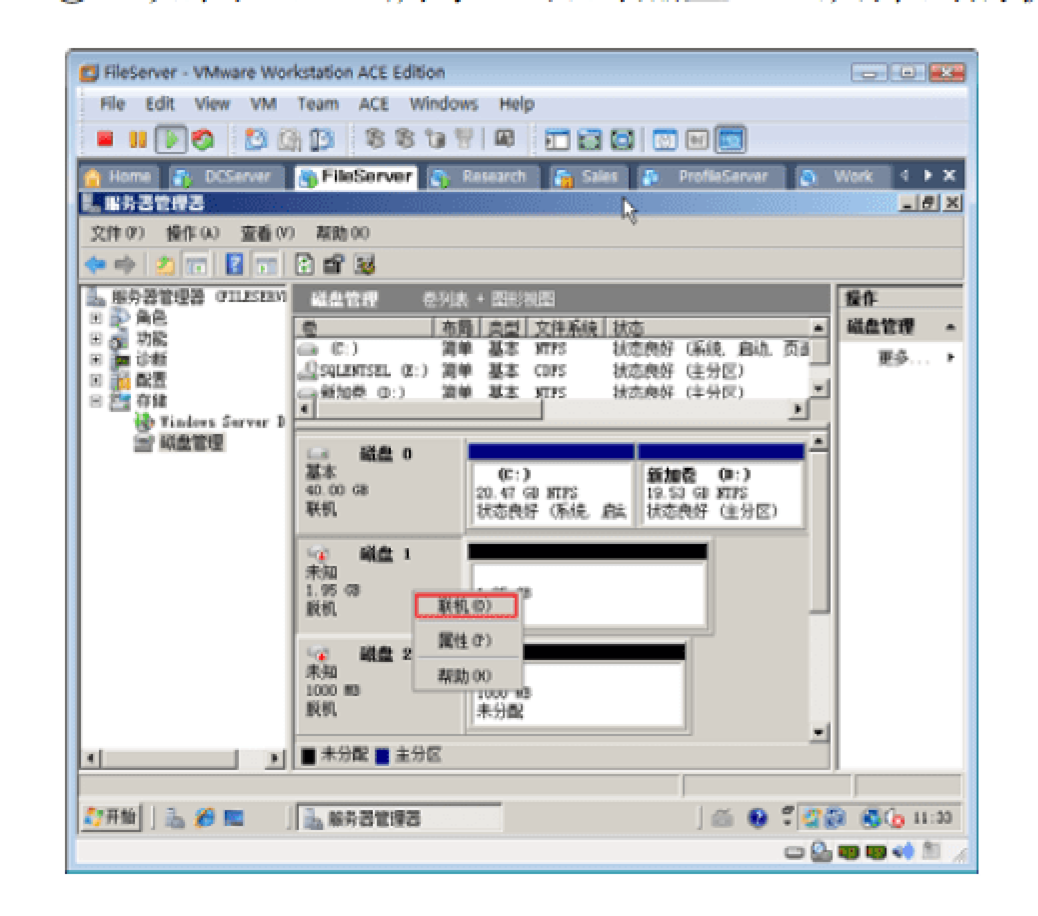


图 15-35　联机磁盘

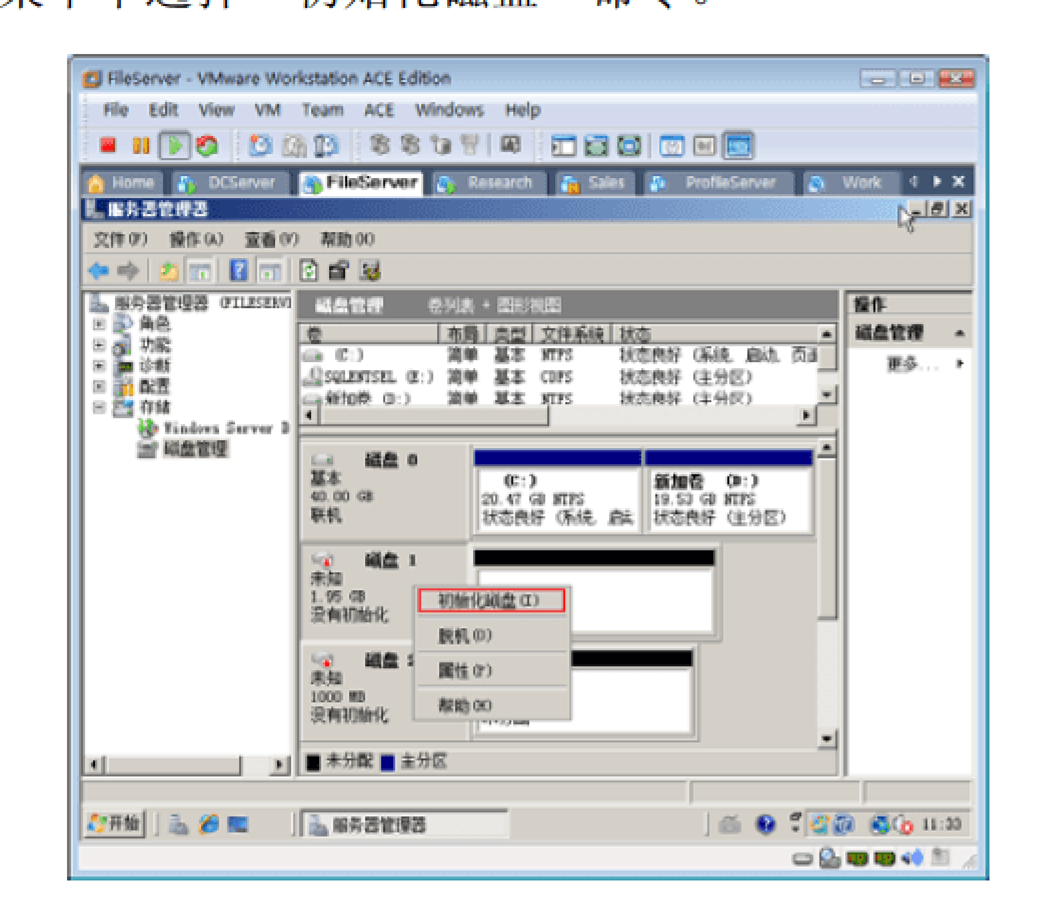


图 15-36　初始化磁盘

⑪　如图 15-37 所示，在出现的“初始化磁盘”对话框中，选中磁盘 1 和磁盘 2，单击“确定”按钮。

⑫　如图 15-38 所示，分区格式为 NTFS 格式，磁盘分区分别为 Q 和 S 盘。

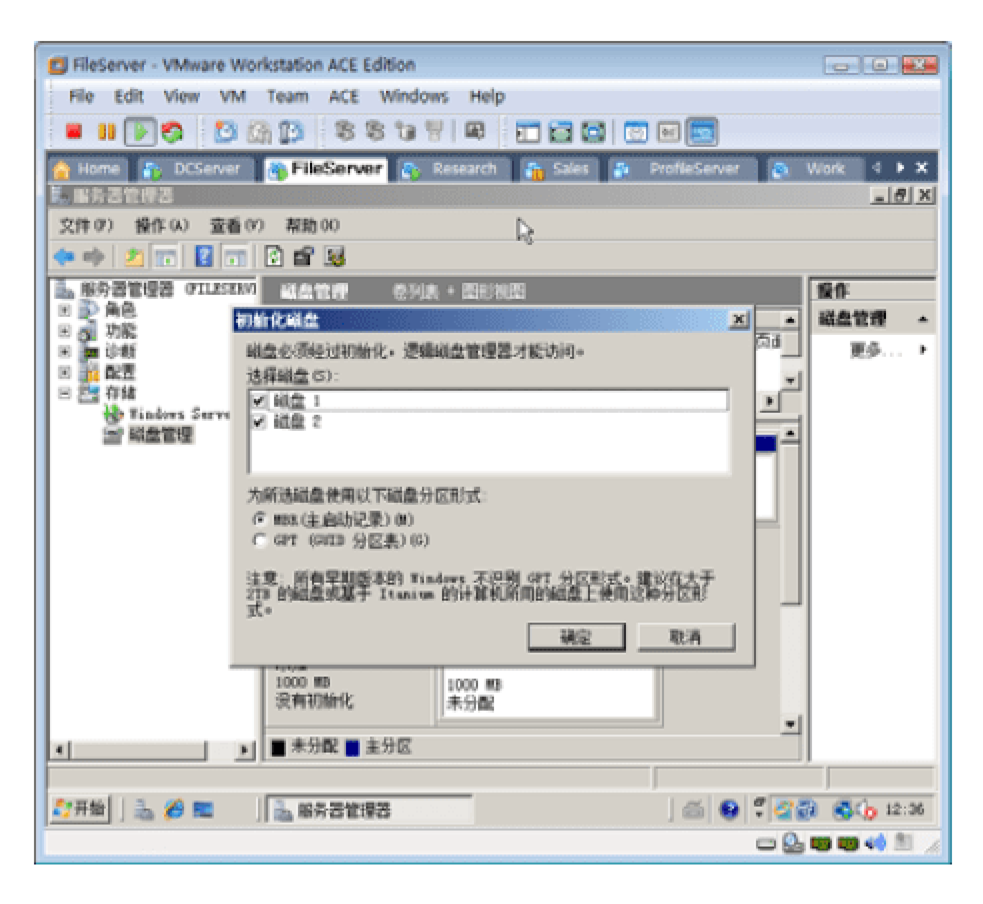


图 15-37　选择初始化磁盘

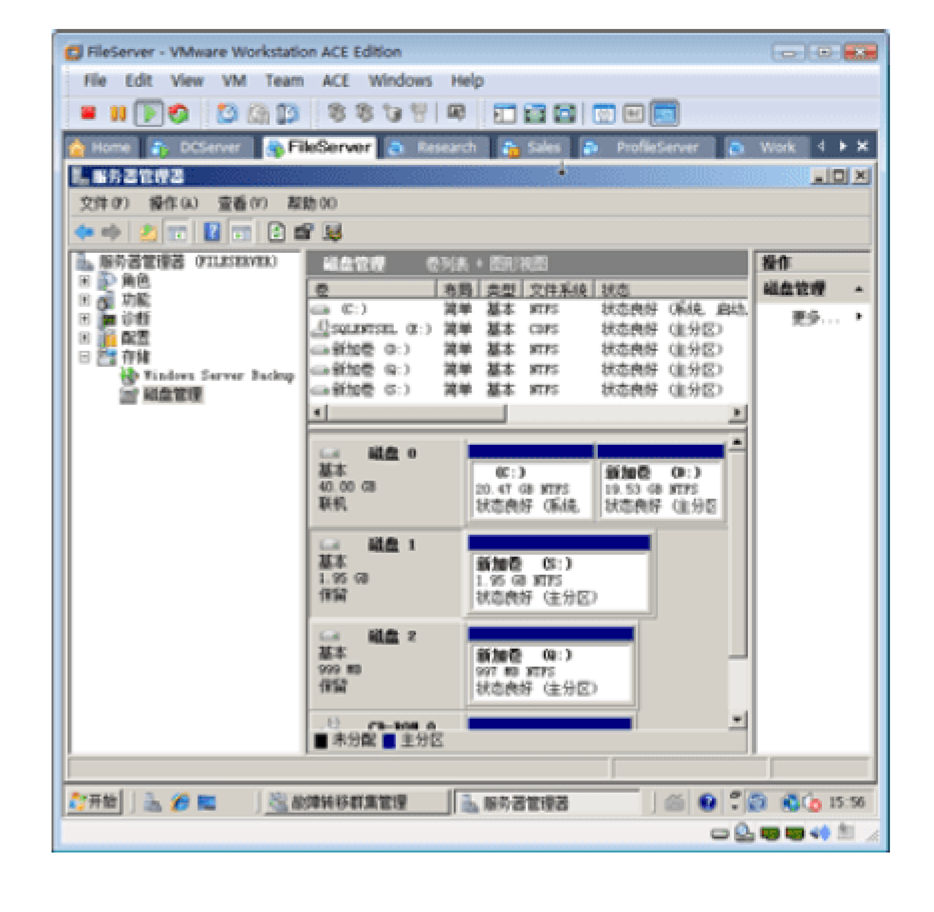


图 15-38　格式化磁盘

15.5.4　在节点 Research 配置 iSCSI

节点 Research 服务器配置 iSCSI 的方法与节点 FileServer 服务器的配置方法完全相同，配置后的结果如图 15-39 所示。在配置过程中，注意将磁盘分区格式设置为 NTFS 格式，分区类型为“基本”。



注意：盘符一定与节点 FileServer 服务器的盘符相同。

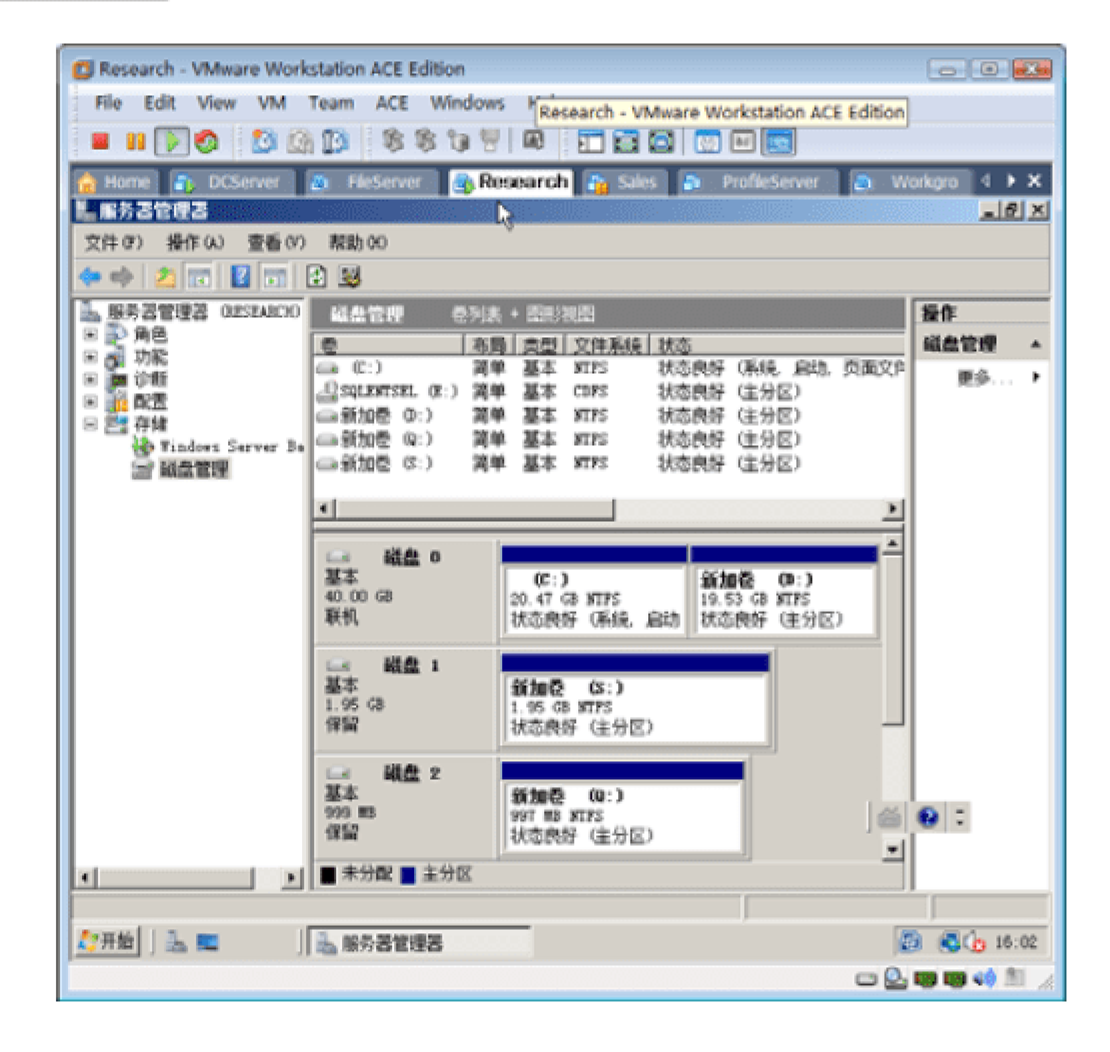


图 15-39　连接 iSCSI 设备

15.6　部 署 群 集

由于本例中使用存储服务，因此节点服务器的开启及关闭不需要遵循以前操作系统版本的群集节点要求，Windows Server 2008 提供有群集部署向导，可以简单、快捷地部署群集。Windows Server 2008 的群集服务对 DHCP、WINS、IIS 等基础服务提供支持。

15.6.1　配置心跳线网络

① 如图 15-40 所示，关闭 FileServer 和 Research，单击 Edit virtual machine settings 选项。

② 如图 15-41 所示，在出现的 Virtual Machine Settings 对话框中，单击 Add 按钮。

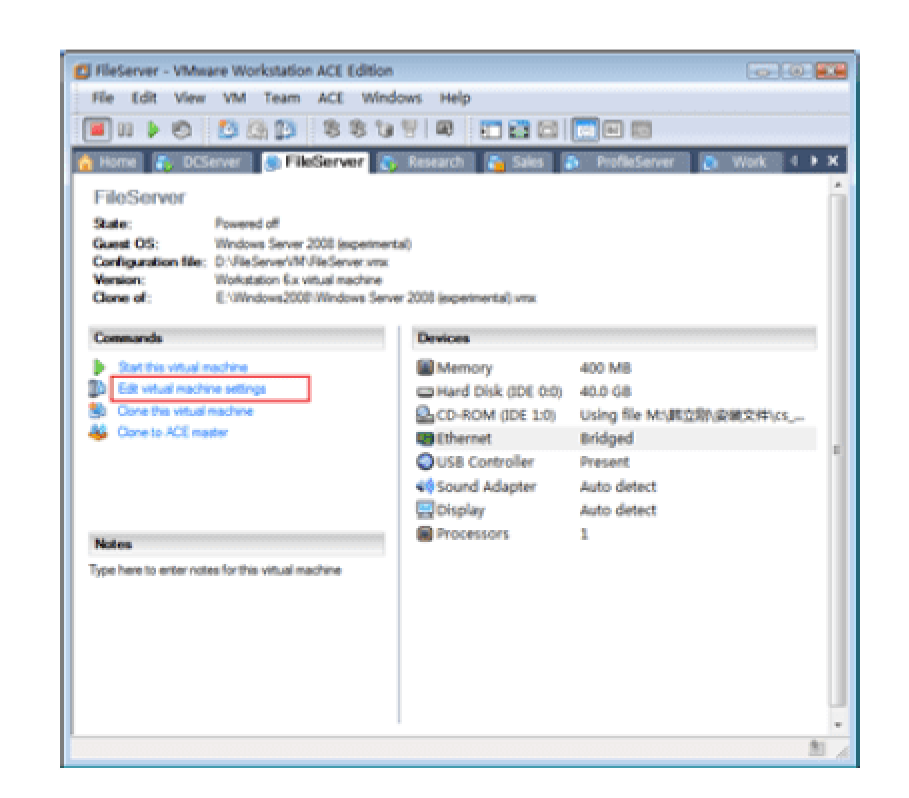


图 15-40　添加设备

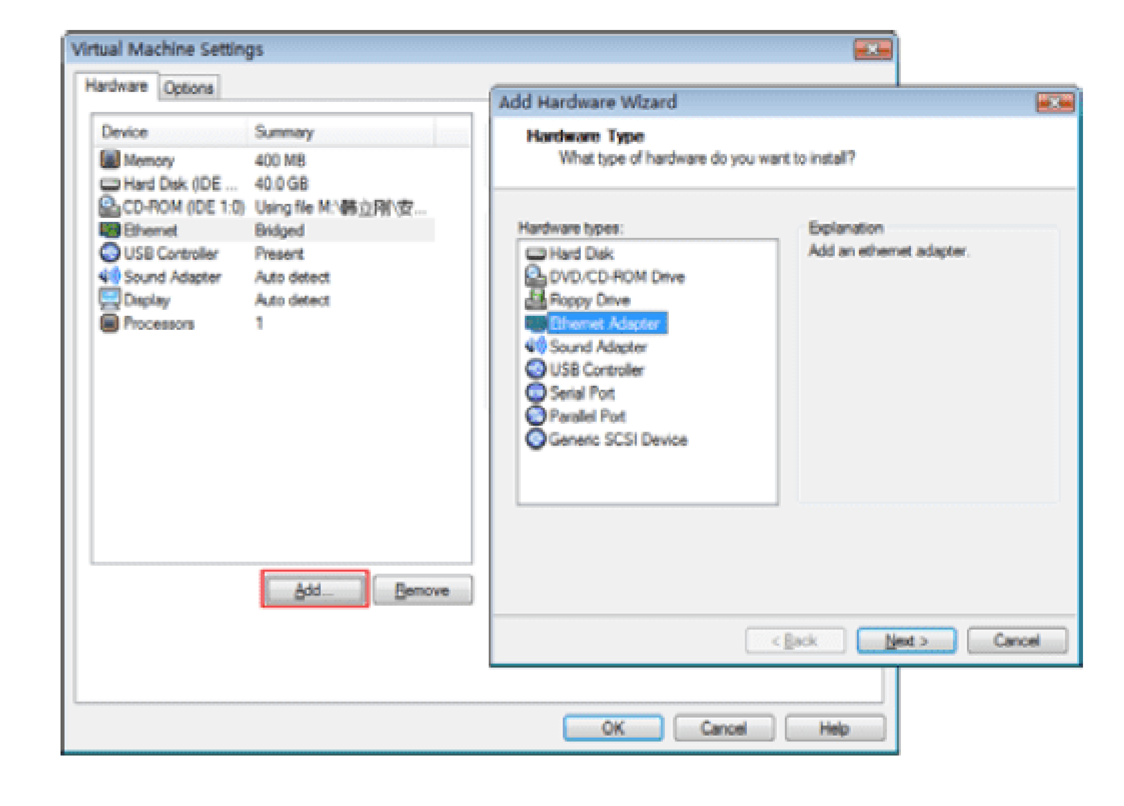


图 15-41　添加网络设备

③ 如图 15-42 所示，在出现的 Network Type 对话框中，选中 Host-only A private network shared with the host，单击 Finish 按钮，可以看到添加了一个网卡，如图 15-43 所示。

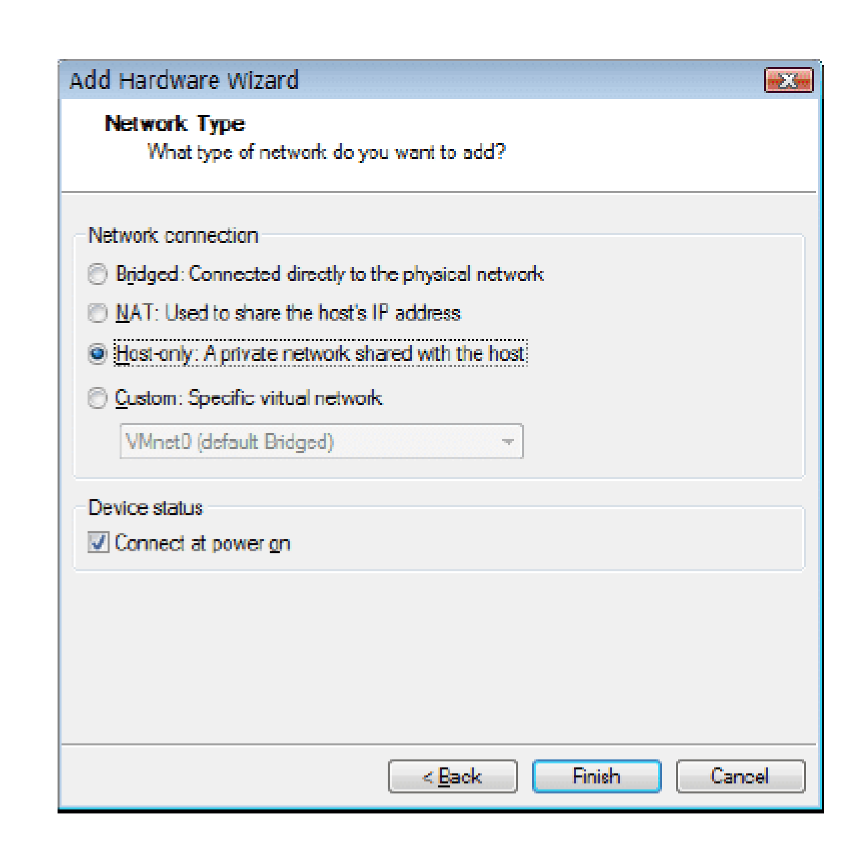


图 15-42　选择网络类型

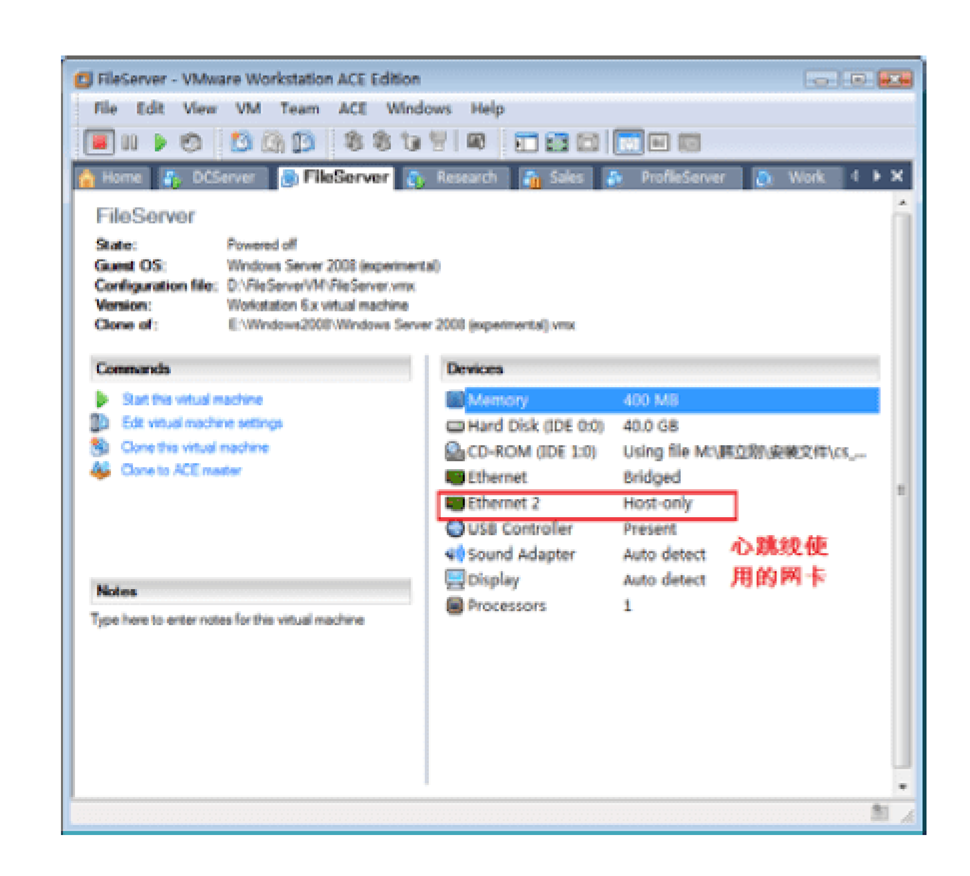


图 15-43　添加的网卡

④　使用相同的方法为 Research 添加一个网卡。

⑤　启动计算机为新添加的网卡添加 IP 地址，Research 的为 172.16.0.4，子网掩码为 255.255.0.0，如图 15-44 所示。FileServer 的为 172.16.0.1，子网掩码为 255.255.0.0，如图 15-45 所示。

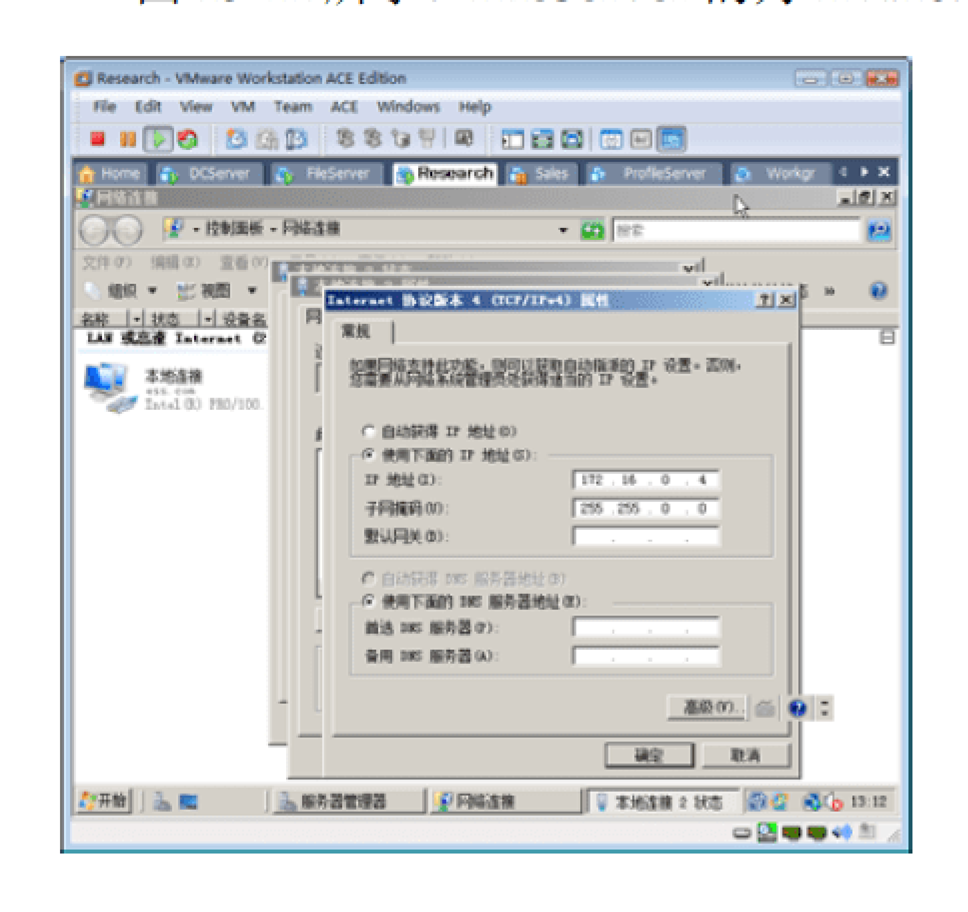


图 15-44　设置心跳线 IP 地址(一)

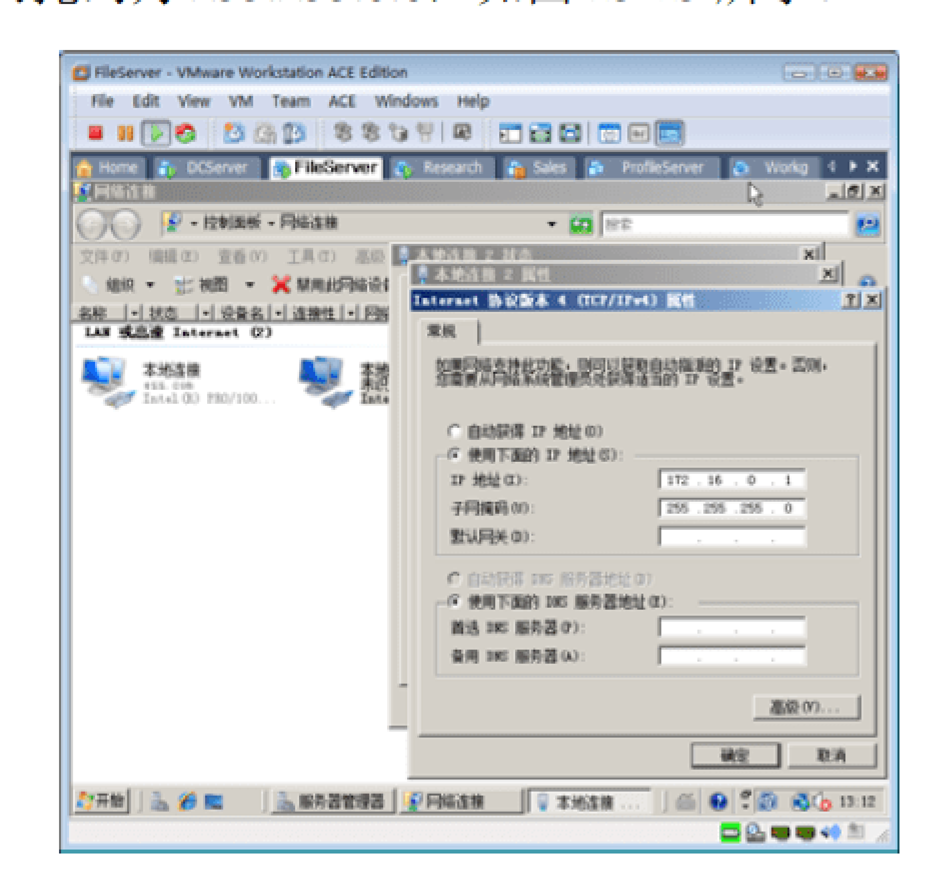


图 15-45　设置心跳线 IP 地址(二)

15.6.2　安装故障转移群集

在安装 Windows Server 2008 时，故障转移群集作为选件安装，需要网络管理员根据需要定制安装。下面介绍故障转移群集的安装方法。

①　选择“开始”→“管理工具”→“服务器管理器”命令，显示如图 15-46 所示的“服务器管理器”窗口。单击“添加功能”按钮，启动添加功能向导。

②　如图 15-47 所示，在“选择功能”界面的“功能列表”中，选择“故障转移群集”选项，单击“下一步”按钮。

③　显示如图 15-48 所示的“确认安装选择”界面中，单击“安装”按钮。

④　如图 15-49 所示，开始安装故障转移群集。安装完成后，显示“安装结果”界面，单击“关闭”按钮，完成故障转移群集的安装。

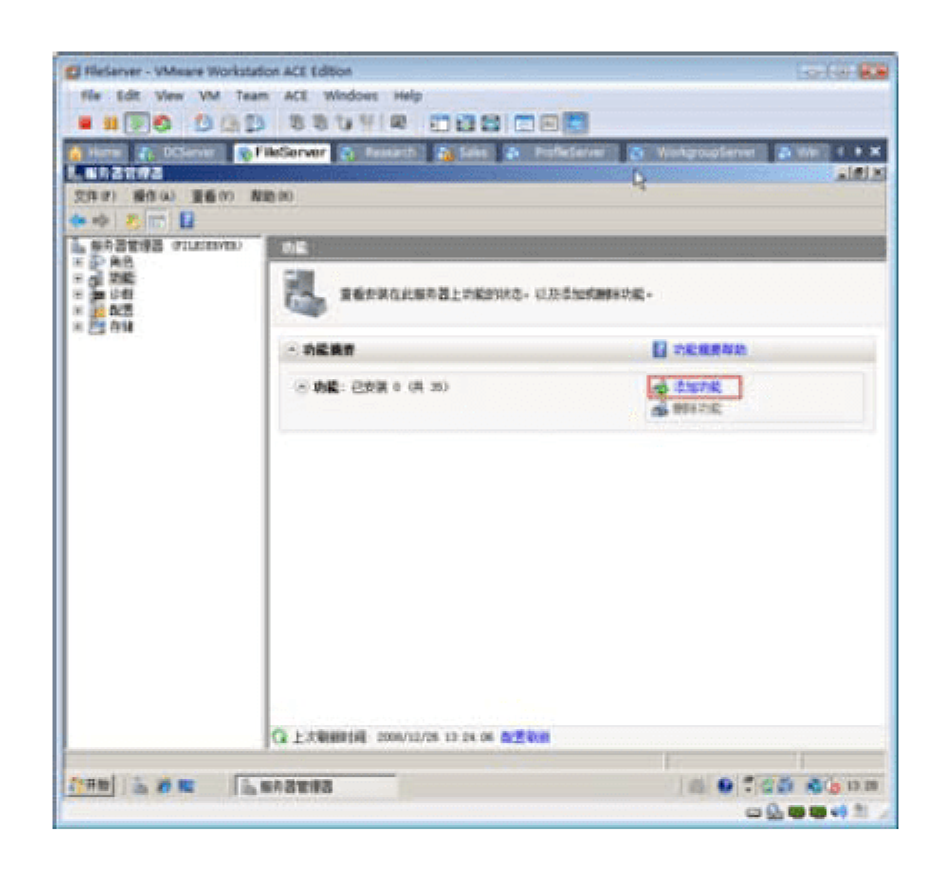


图 15-46　添加功能

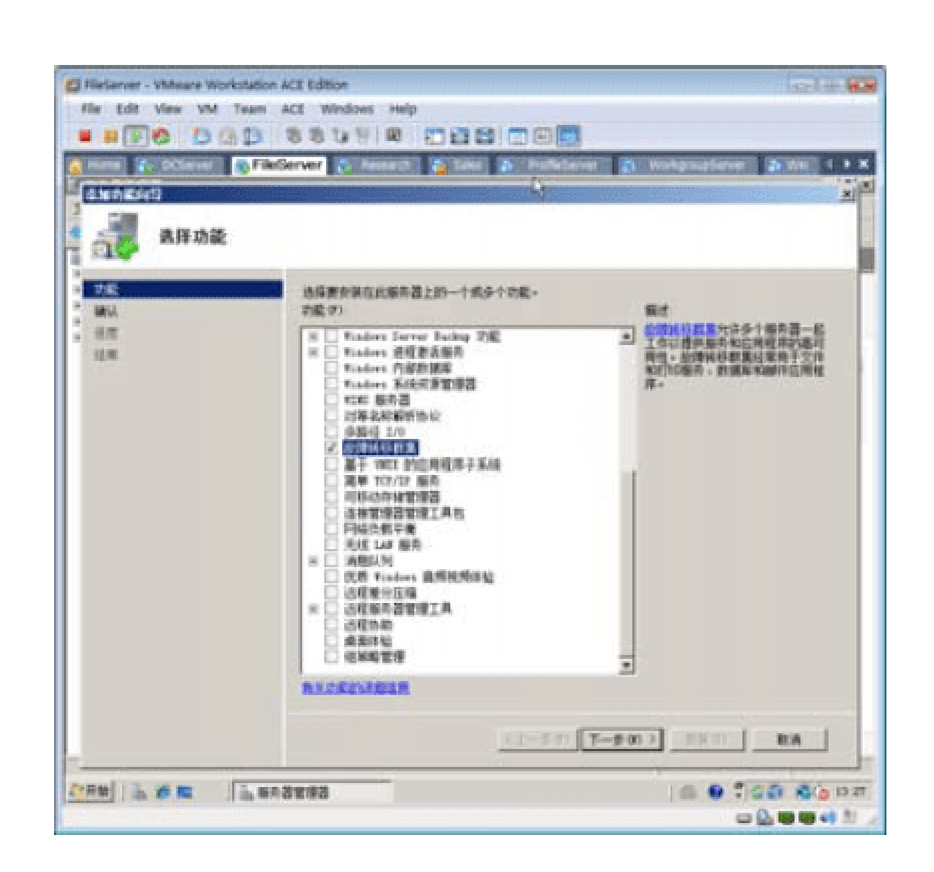


图 15-47　选择功能

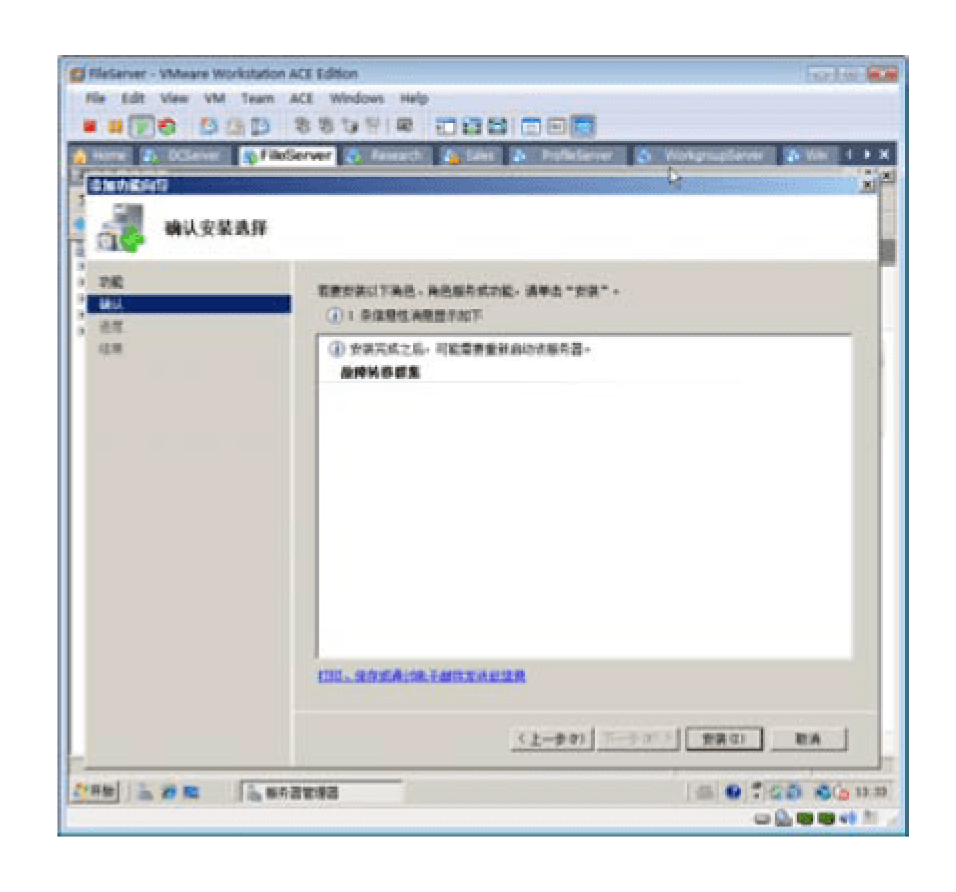


图 15-48　安装功能

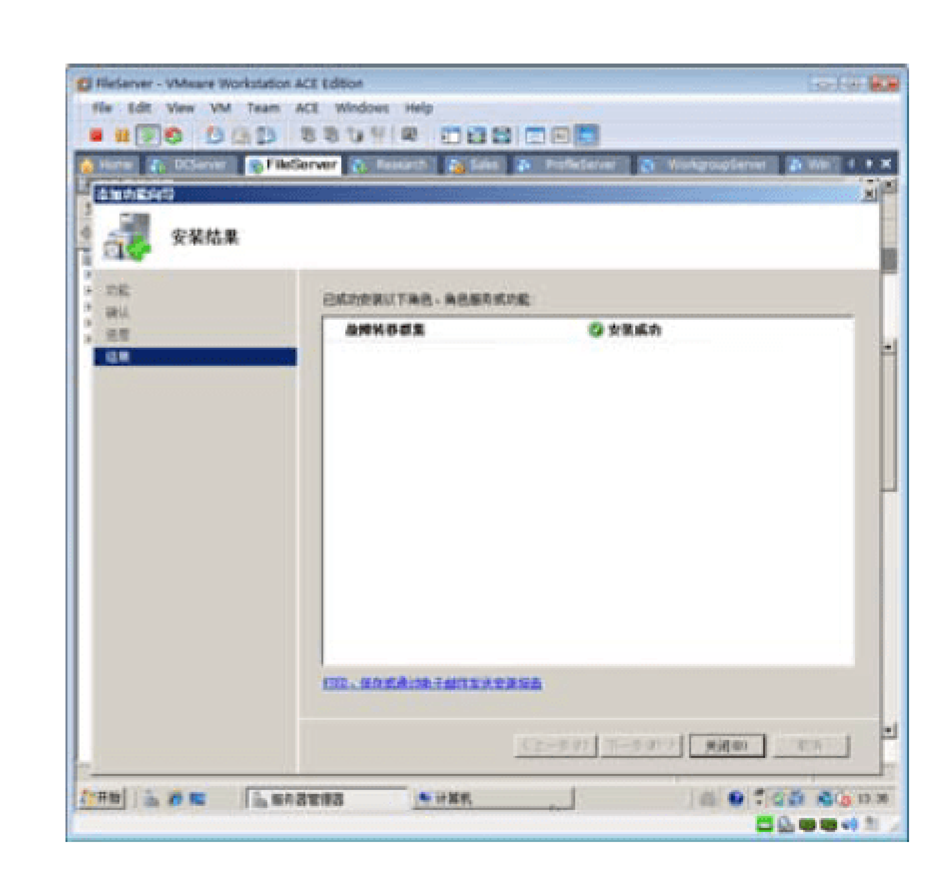


图 15-49　完成安装

⑤　在节点 Research 安装故障转移群集。

⑥　如图 15-50 所示，在 DCServer 上，打开 StarWind 软件，可以看到群集节点 FileServer 和 Research 服务器已经连接到创建的虚拟磁盘中。

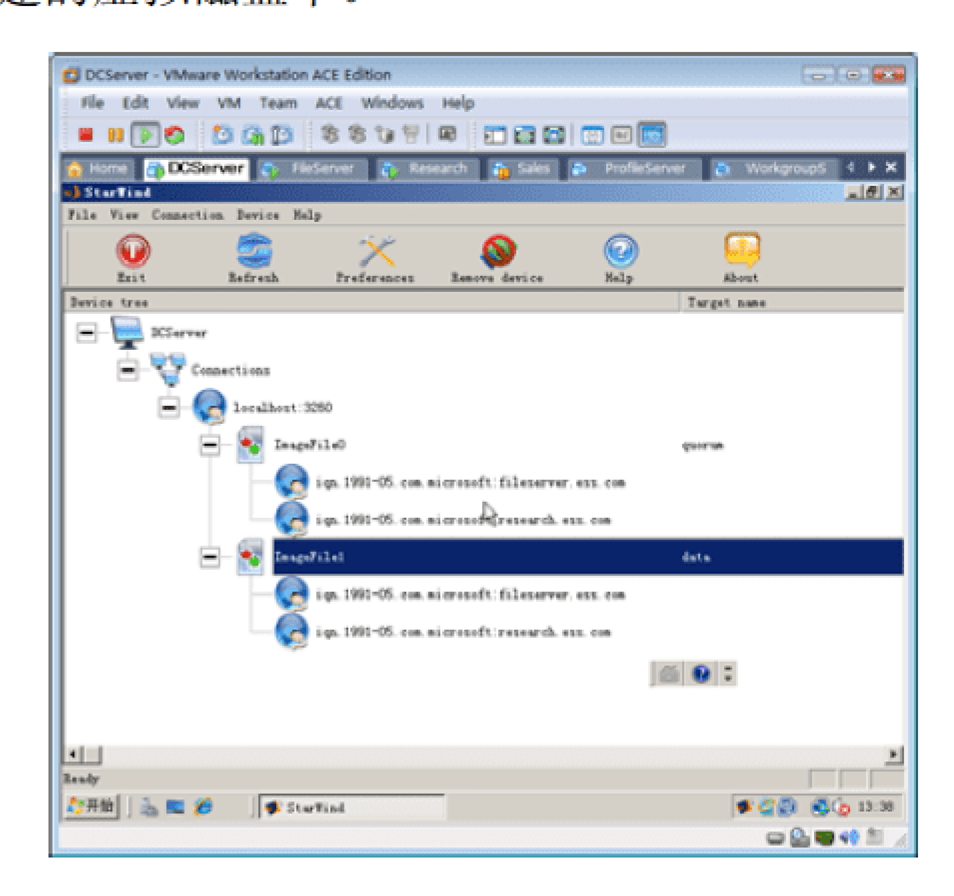


图 15-50　查看连接的计算机

15.6.3　创建群集

创建群集之前，所有的节点服务器均需要开启。在任何一台节点服务器中，都可以部署群集。创建群集的服务器就是群集的所有者。

① 在节点 FileServer 服务器中，选择“开始”→“管理工具”→“故障转移群集管理”命令，显示如图 15-51 所示的“故障转移群集管理”窗口。

② 单击“创建一个群集”超链接，启动“创建群集向导”，显示如图 15-52 所示。

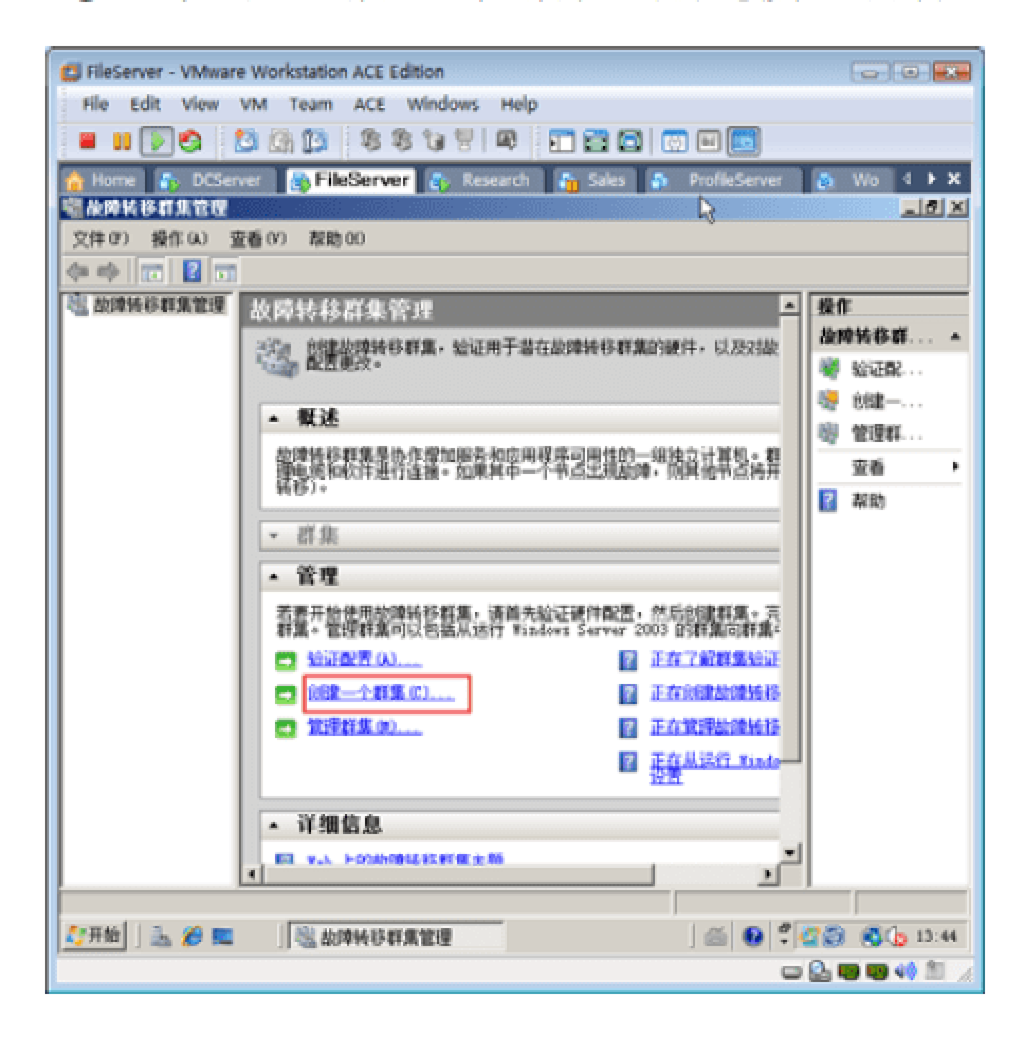


图 15-51　创建一个群集

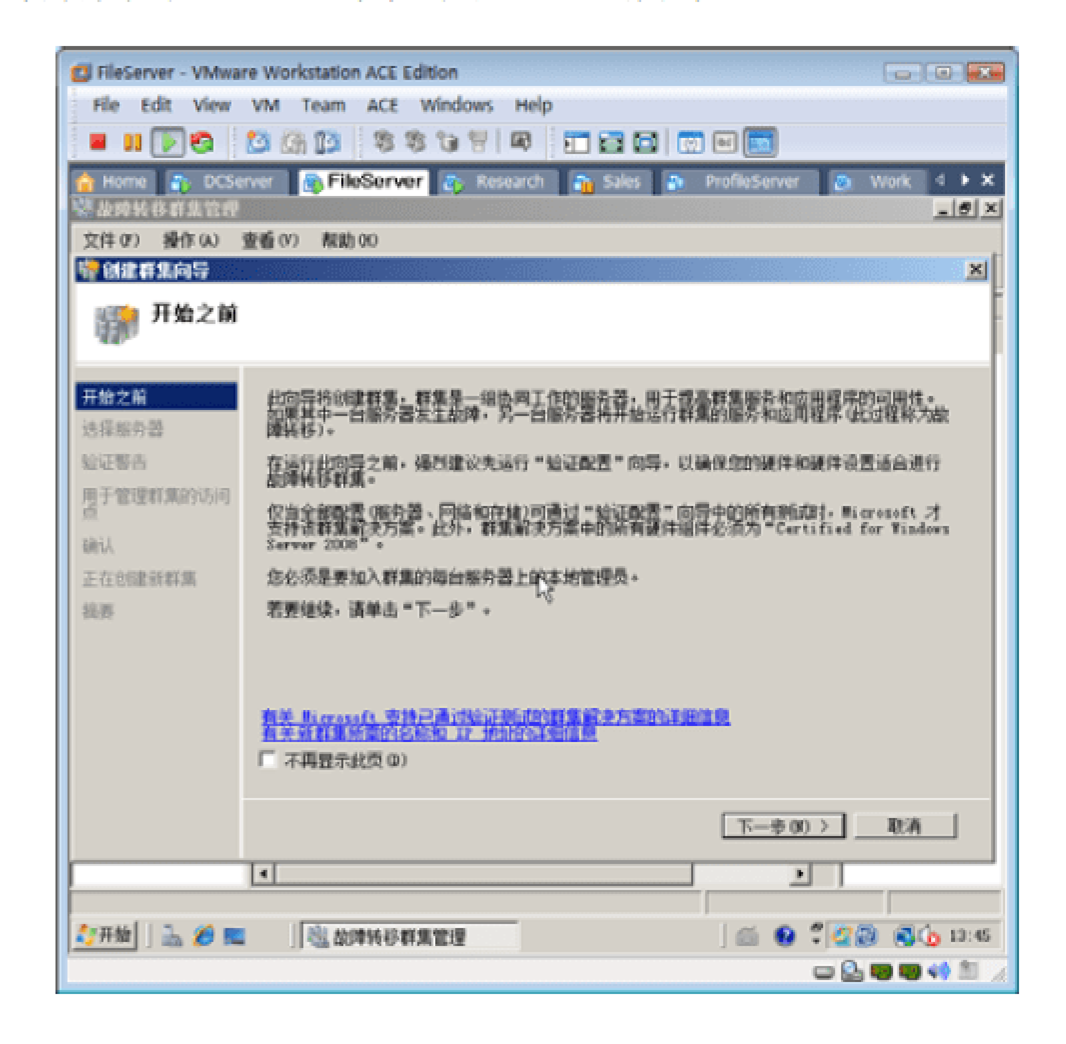


图 15-52　创建群集向导

③ 如图 15-53 所示，在“请选择服务器或群集”界面中，输入 FileServer，单击“添加”按钮，输入 research，单击“添加”按钮。单击“下一步”按钮。

④ 如图 15-54 所示，在“正在测试选项”界面中，选中“运行所有测试”单选按钮，单击“下一步”按钮。

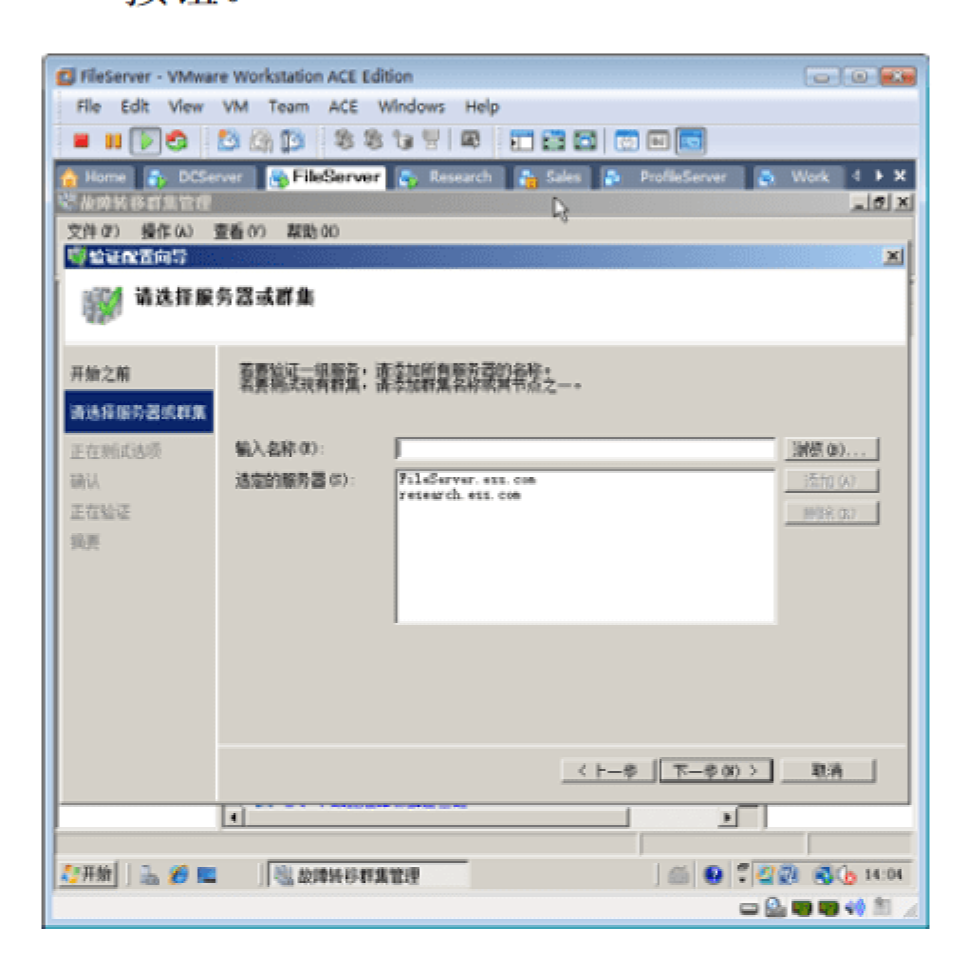


图 15-53　添加两个节点

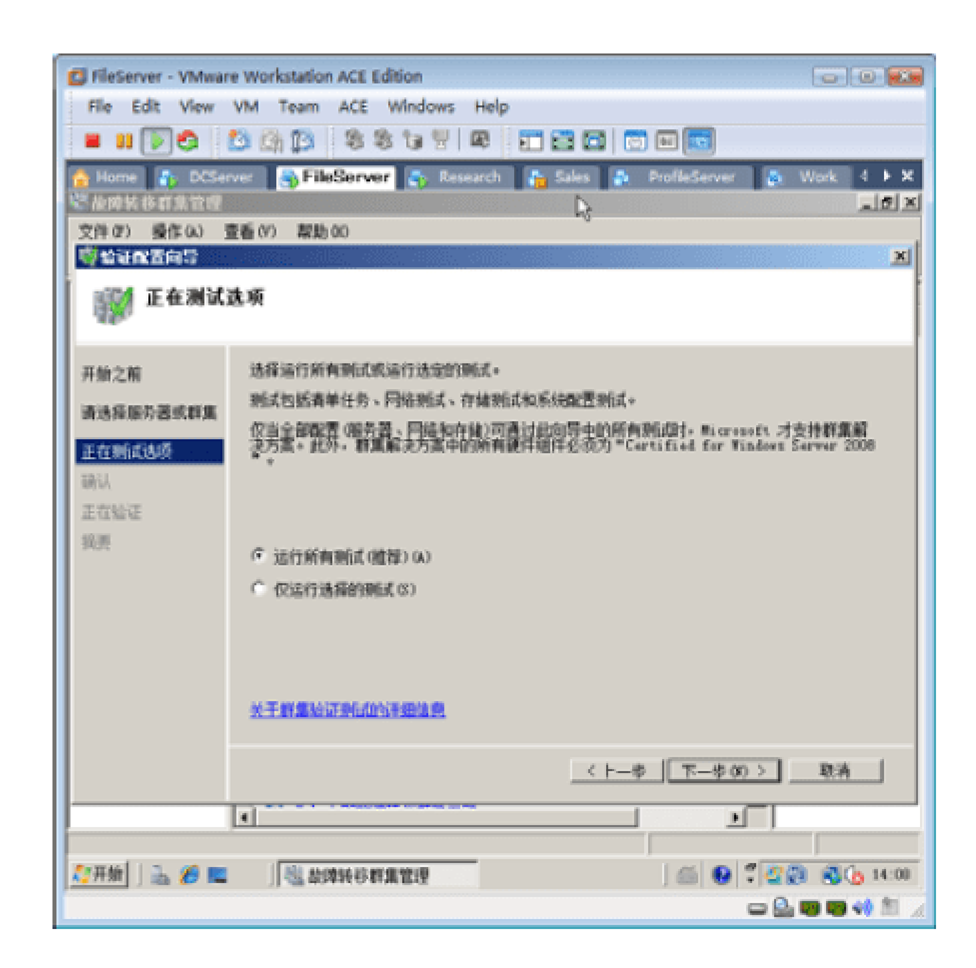


图 15-54　进行测试

⑤ 如图 15-55 所示，在“确认”界面中，单击“确认”按钮。

⑥ 如图 15-56 所示，在“正在验证”界面中，开始测试选择的节点服务器。

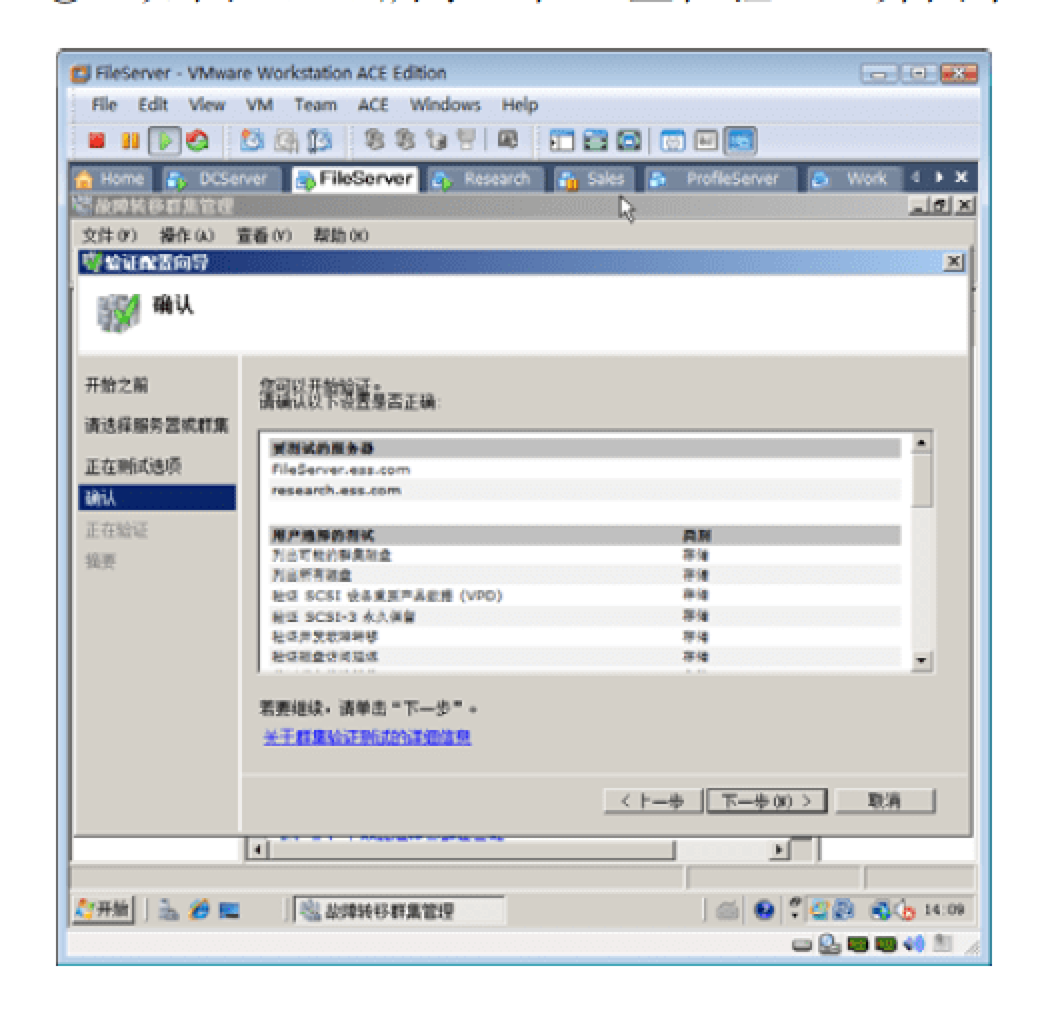


图 15-55 确认

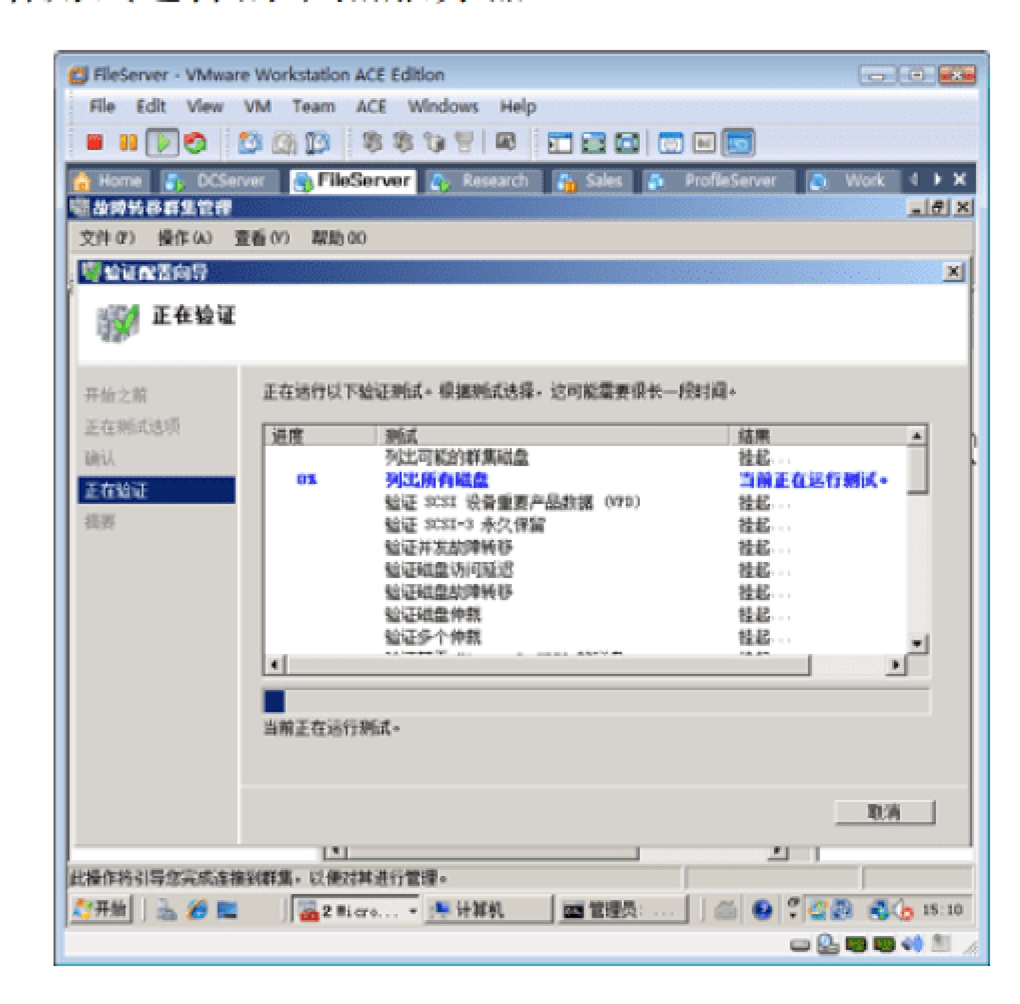


图 15-56 验证

⑦ 测试完成后，显示如图 15-57 所示的“摘要”界面，选择的节点服务器适合安装群集。单击“完成”按钮，关闭“摘要”界面，返回到“创建群集向导”。

⑧ 如图 15-58 所示，在出现的“用于管理群集的访问点”界面中，在“群集名称”文本框中输入群集的名称，在“地址”文本框中输入群集使用的 IP 地址，单击“下一步”按钮。

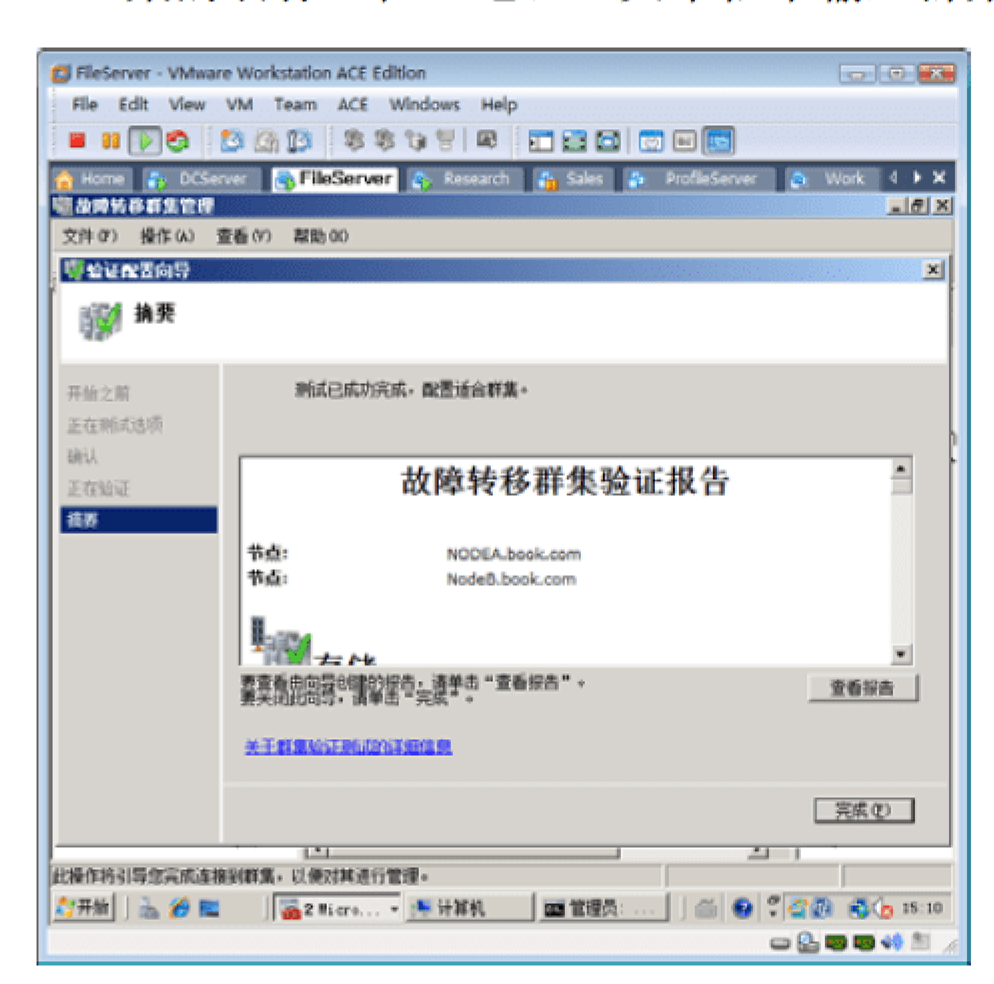


图 15-57 完成验证

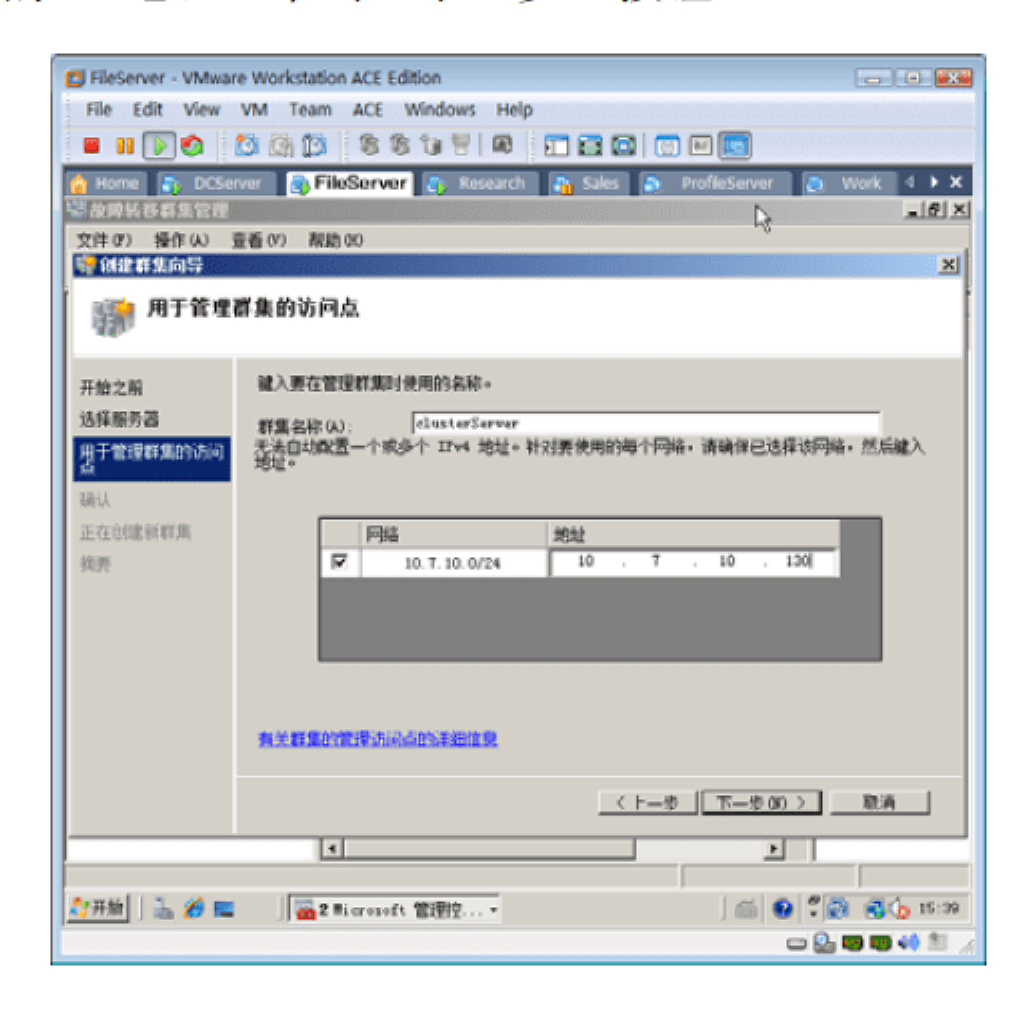


图 15-58 输入群集 IP 地址

⑨ 显示如图 15-59 所示的“确认”界面。

⑩ 启动群集配置进程，显示如图 15-60 所示的“正在创建新群集”界面。

⑪ 配置完成后，显示如图 15-61 所示的“摘要”界面，显示已经成功创建群集。

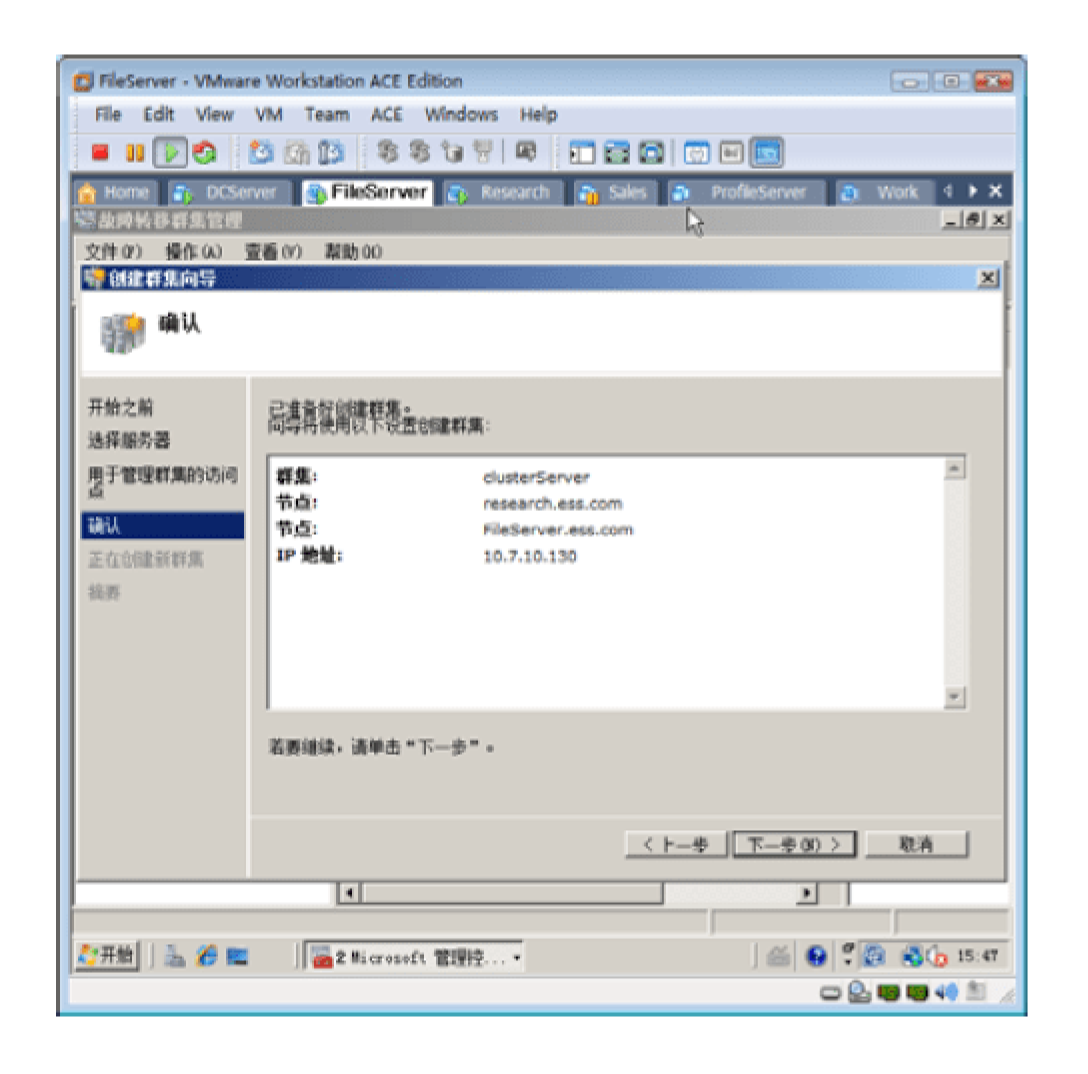


图 15-59　确认

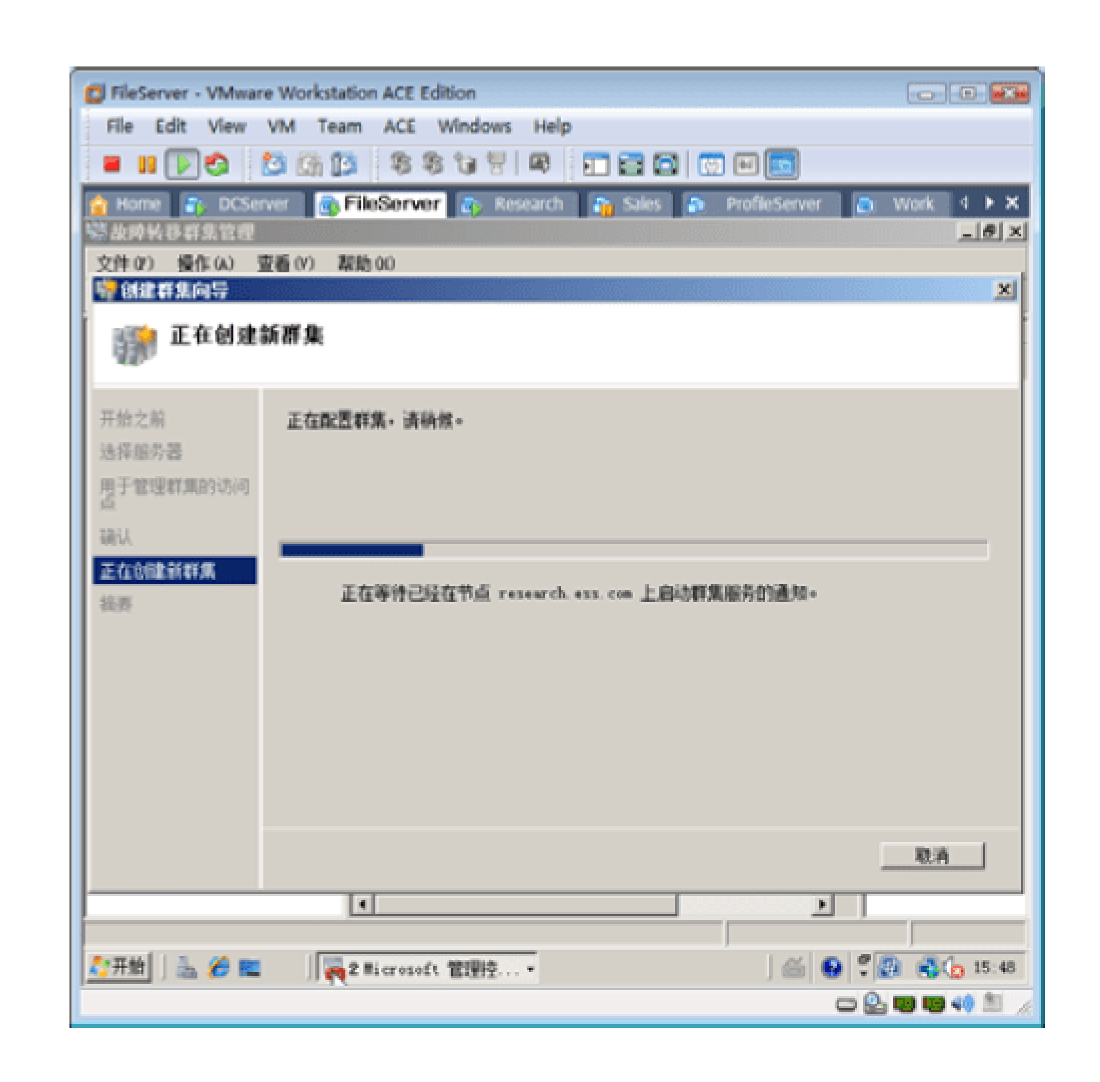


图 15-60　正在创建新群集

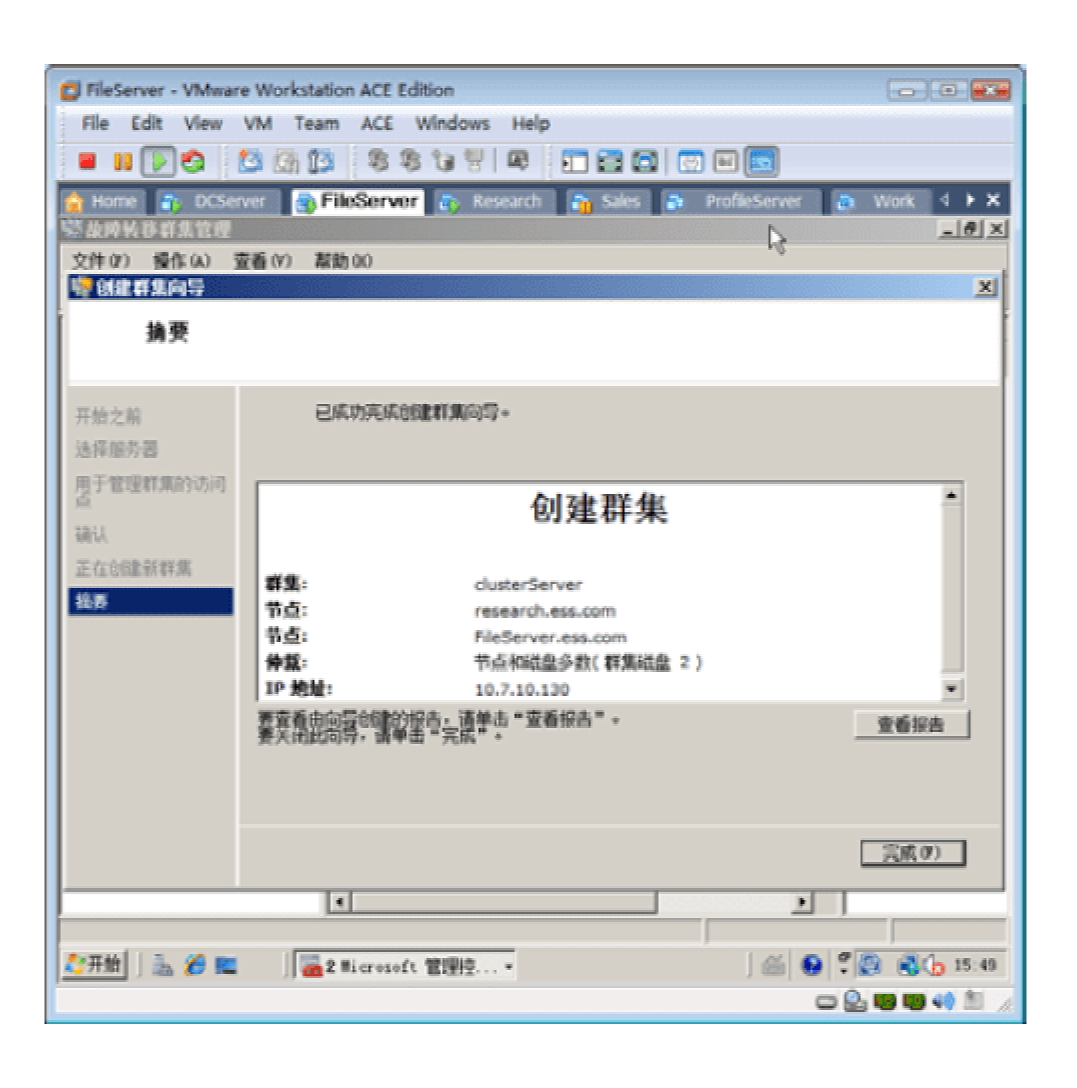


图 15-61　完成群集创建

15.6.4　验证群集配置

① 在 FileServer 上，打开故障转移群集管理工具，如图 15-62 所示，单击 clusterServer.ess.com，可以看到当前主服务器是 FileServer。

② 如图 15-63 所示，在命令行下，输入 ipconfig 可以看到群集地址 10.7.10.130。

③ 如图 15-64 所示，在 FileServer 上，打开计算机，可以看到 Q 分区和 S 分区。

④ 如图 15-65 所示，在 Research 上，打开“服务器管理器”窗口，单击“磁盘管理”选项，可以看到磁盘的控制权不在 Research 节点上。

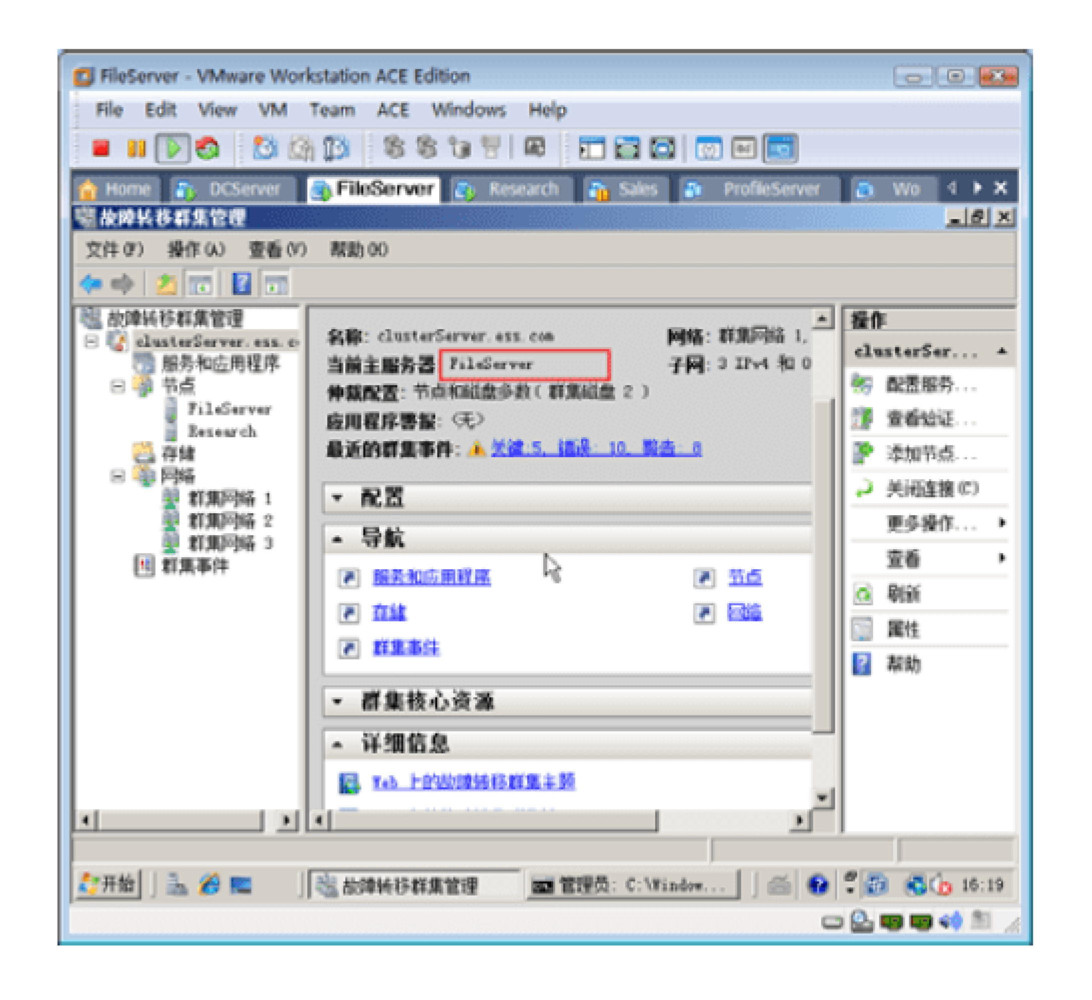


图 15-62　看到当前主服务器

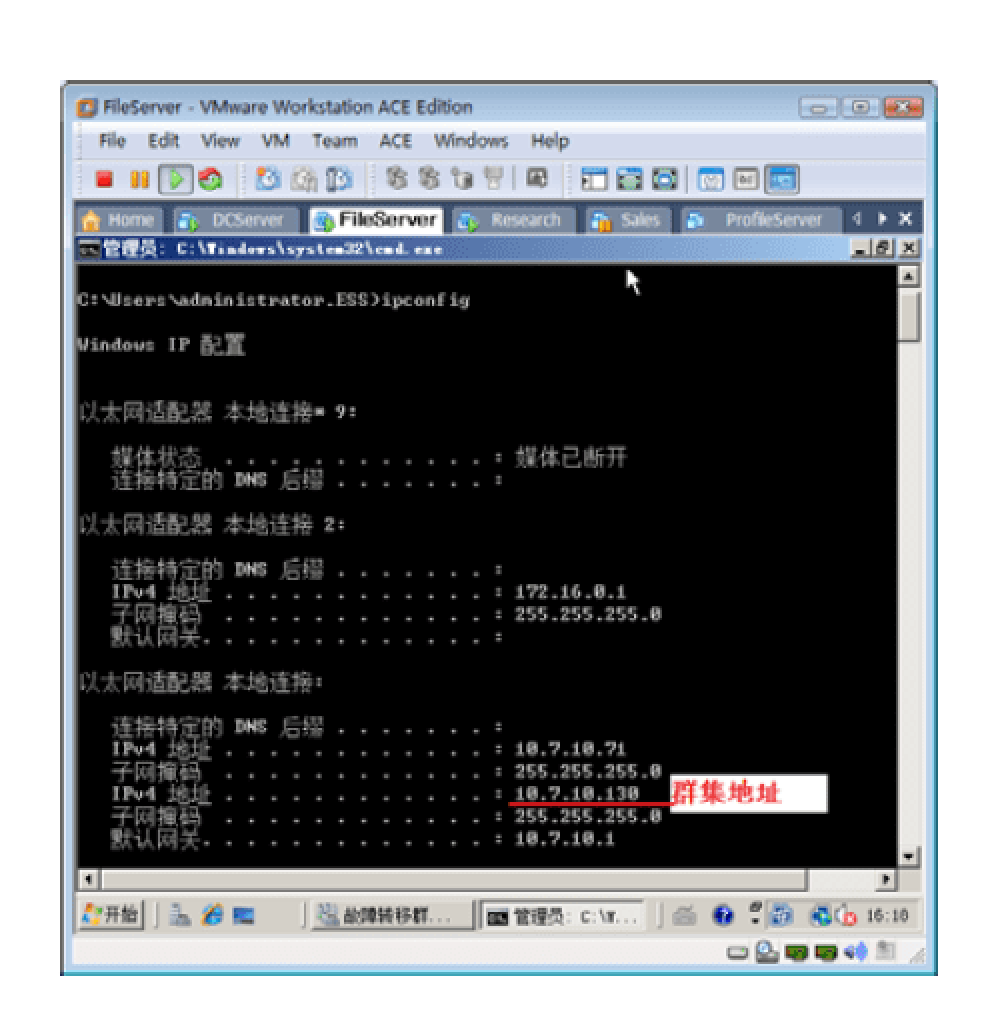


图 15-63　群集 IP 地址

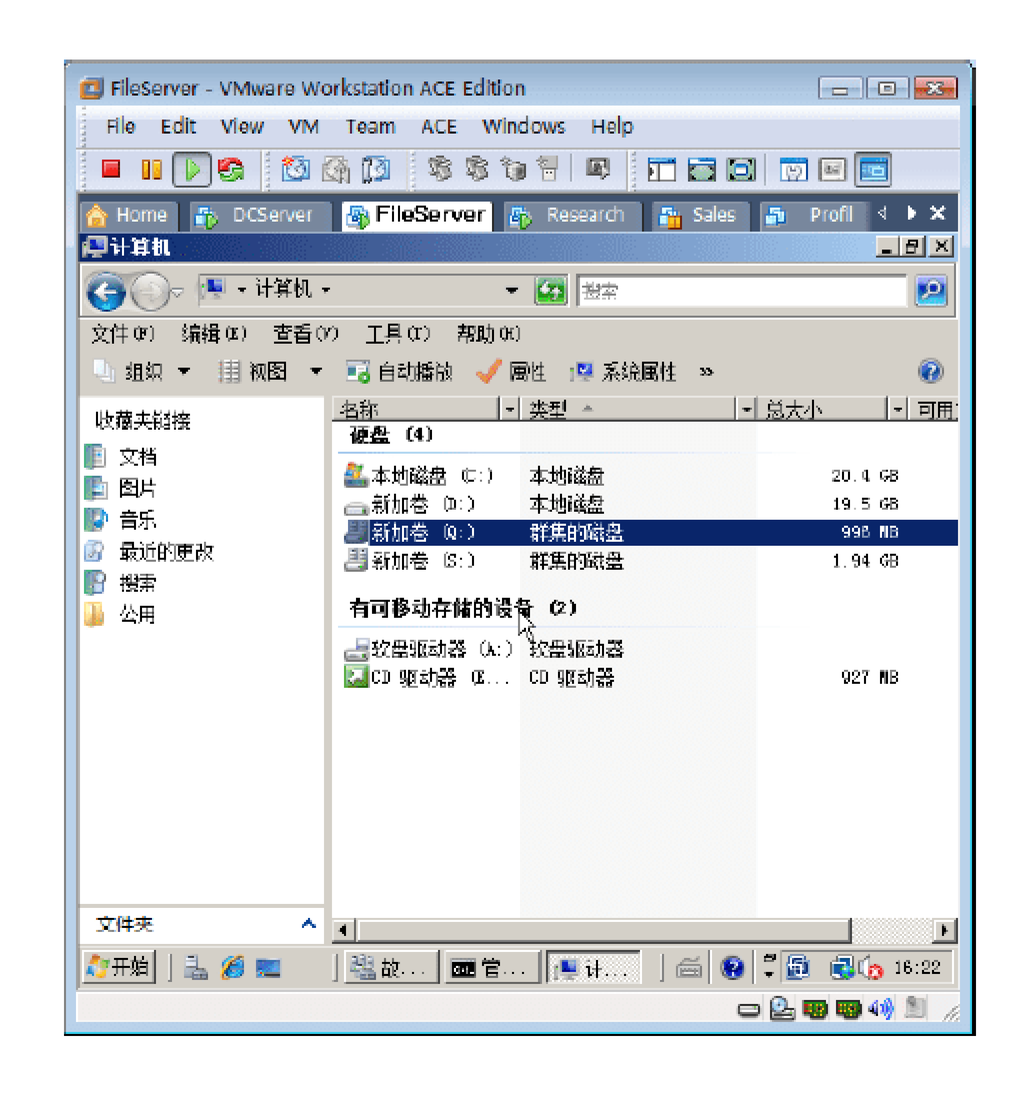


图 15-64　磁盘的控制权

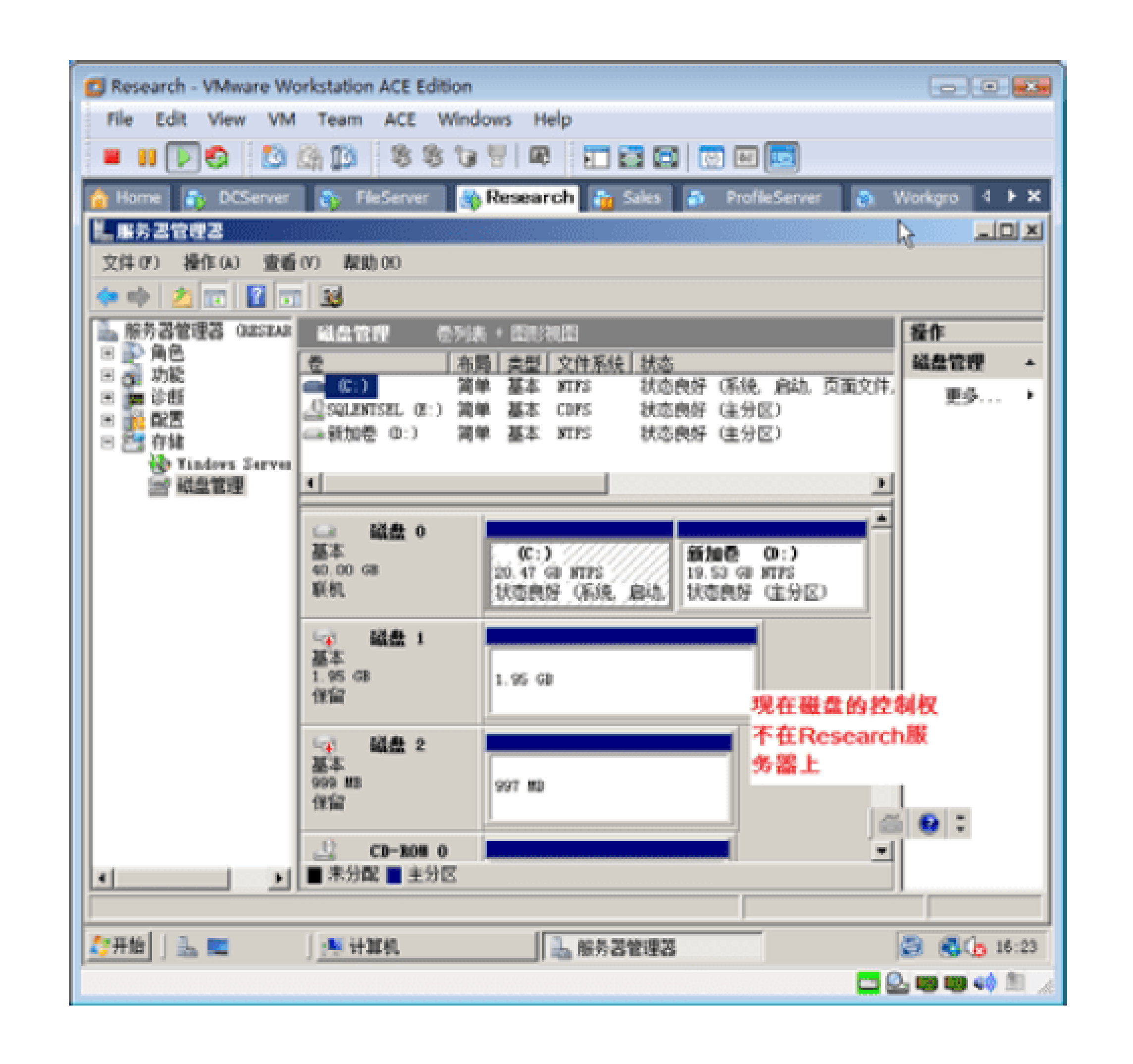


图 15-65　控制权不在该节点

15.6.5　测试故障转移

以下操作将会模拟 FileServer 节点失败后，检测群集的故障转移。

① 在 FileServer 上，打开故障转移群集管理工具，如图 15-66 所示，右击 FileServer，从弹出的快捷菜单中选择“更多操作”→“停止群集服务”命令。

② 如图 15-67 所示，在出现的确认对话框中，单击“停止 FileServer 上的群集服务”按钮。

③ 如图 15-68 所示，可以看到 Research 节点已经接管了磁盘的控制权，并且能够打开。

④ 在命令行下输入 ipconfig，能够看到群集地址已经绑定到 Research 节点，如图 15-69 所示。

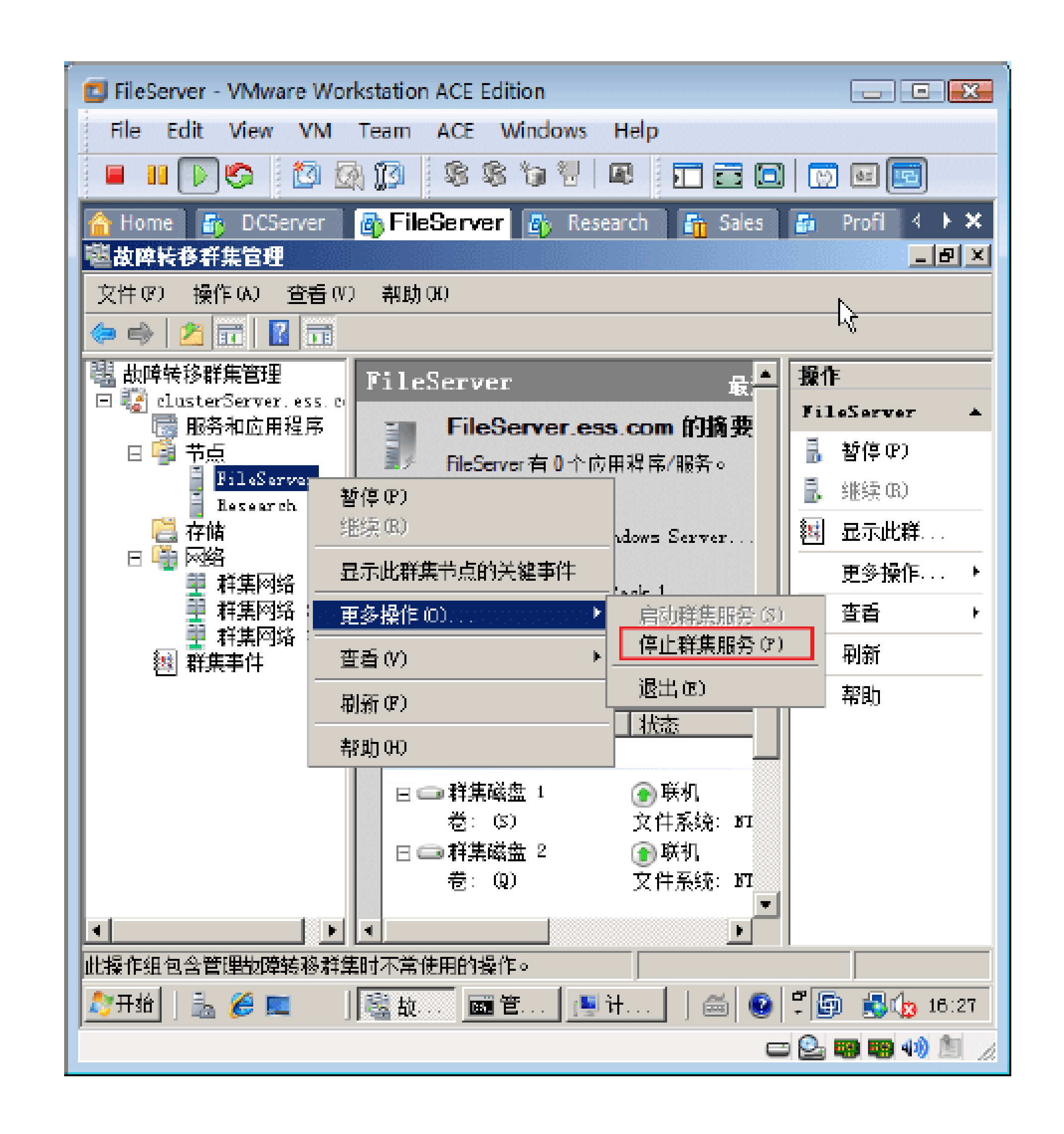


图 15-66　选择“停止群集服务”命令

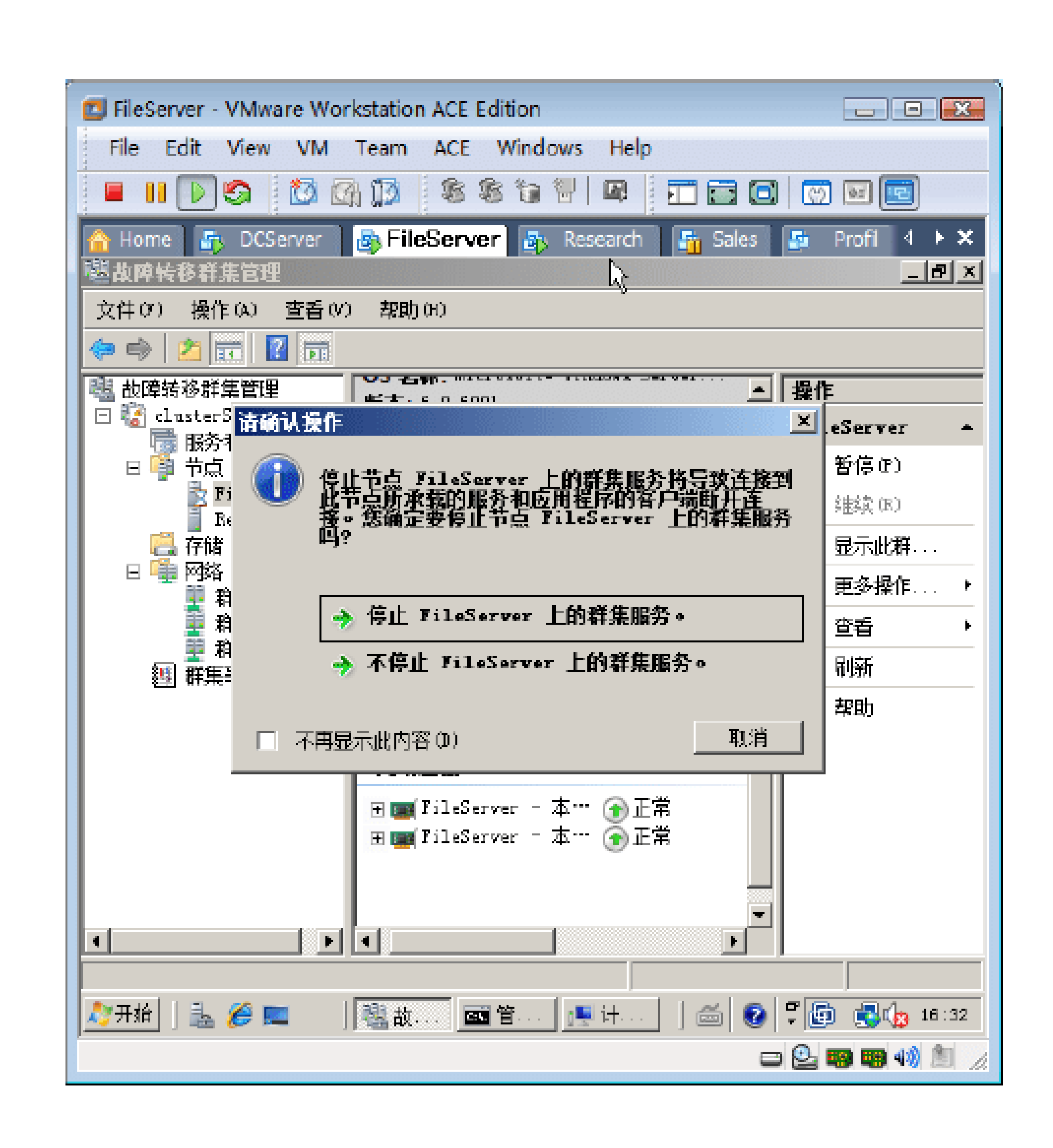


图 15-67　停止群集服务

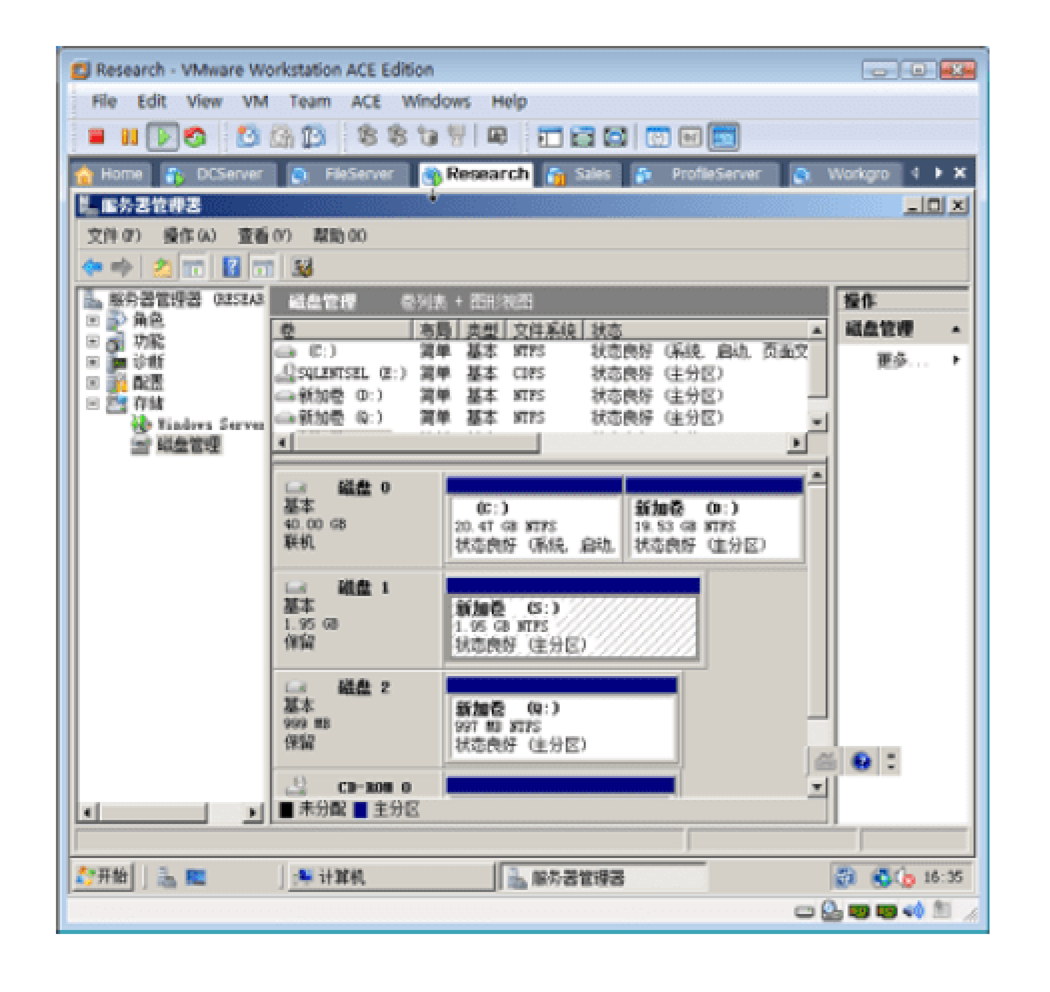


图 15-68　群集切换到另外一个节点

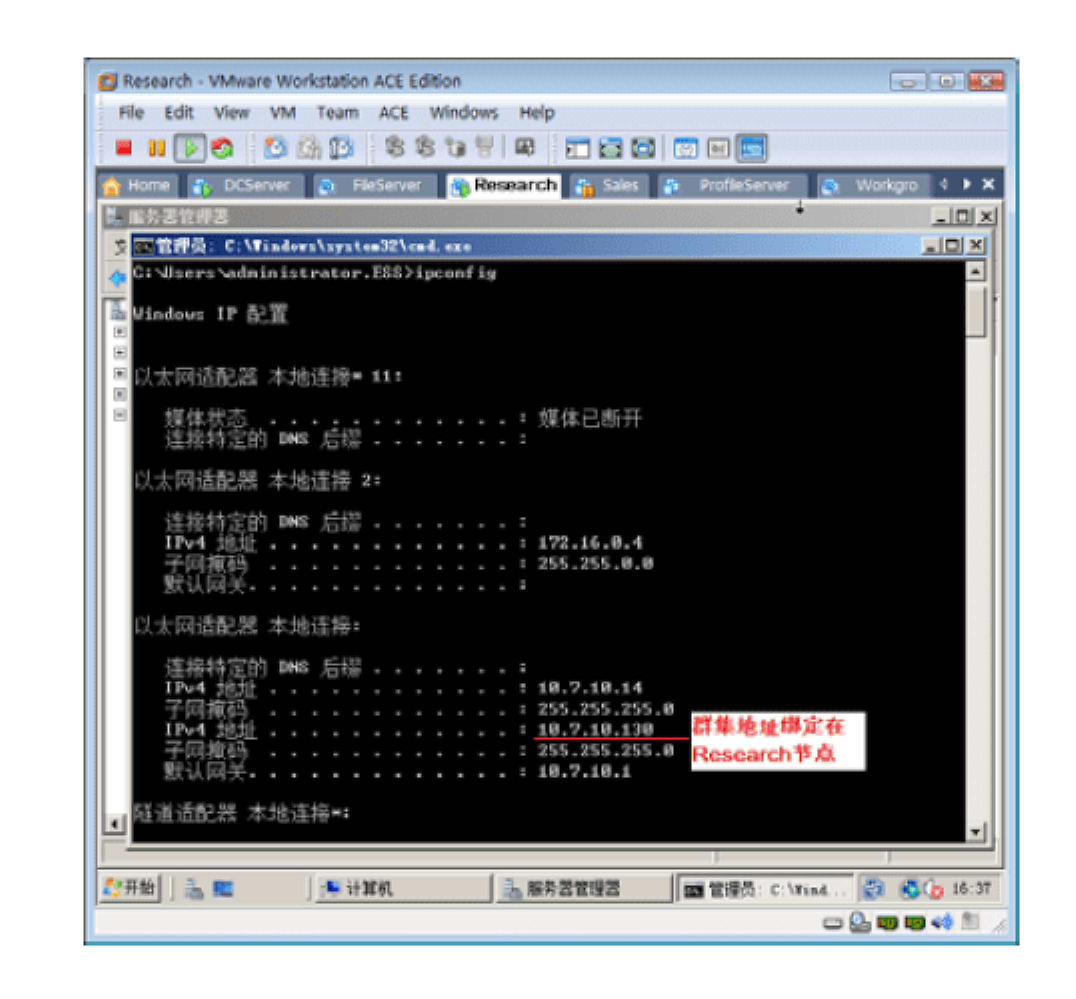


图 15-69　群集 IP 地址绑定到该节点

15.6.6　删除或添加群集节点

可以在配置好的群集中添加或删除节点，操作如下。

① 如图 15-70 所示，打开故障转移群集管理工具，右击群集中的节点 Research，在弹出的快捷菜单中选择“更多操作”→“退出”命令。

② 如图 15-71 所示，在出现的“请确认操作”对话框中，单击“收回节点 Research”按钮。

③ 如图 15-72 所示，退出群集中最后一个节点，会提示退出失败，提示使用命令删除群集。

④ 如图 15-73 所示，在命令提示符下，输入 cluster /destroy，输入 Y，确认操作。

⑤ 如图 15-74 所示，右击节点，在弹出的快捷菜单中选择“添加节点”命令，向群集中添加节点。

⑥ 如图 15-75 所示，在出现的“开始之前”界面中，单击“下一步”按钮。

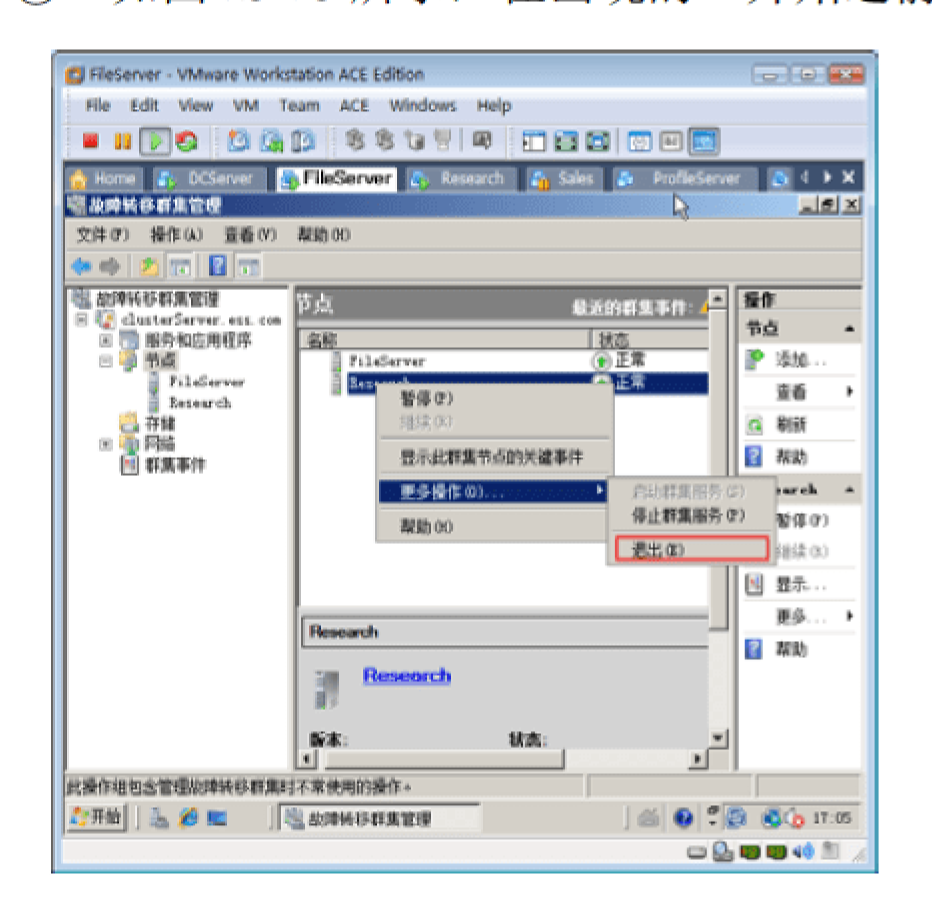


图 15-70 退出节点

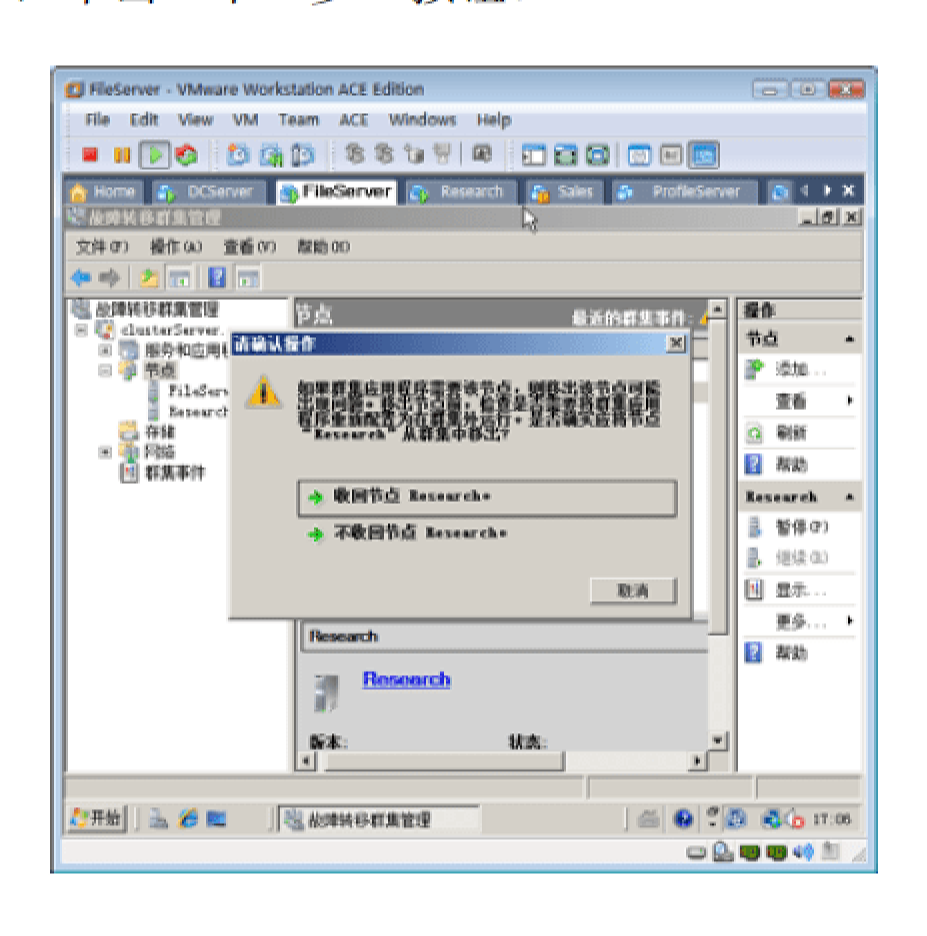


图 15-71 收回节点

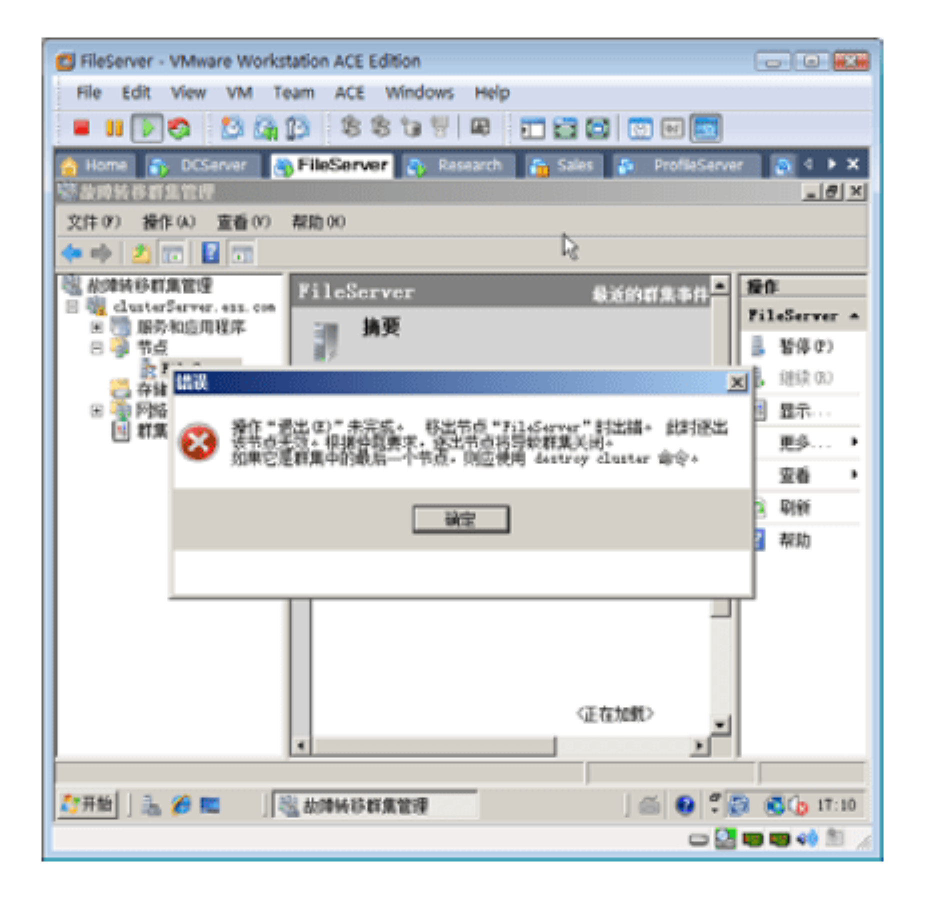


图 15-72 退出节点失败

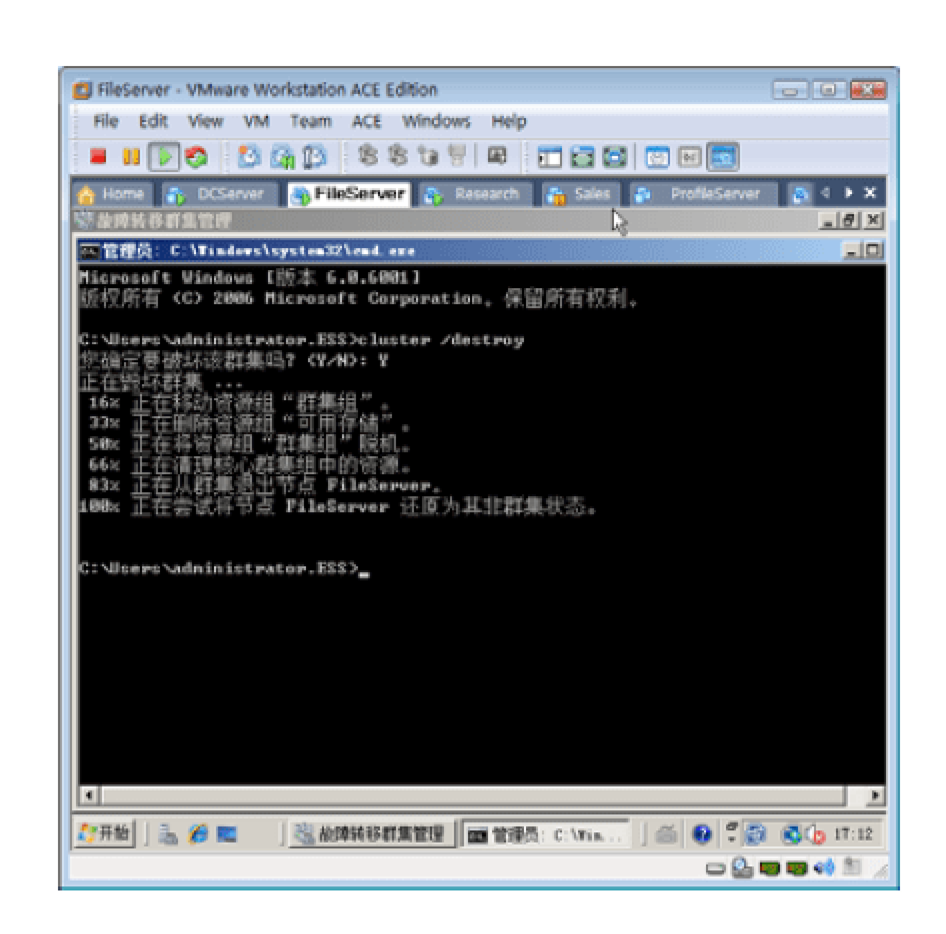


图 15-73 删除最后一个群集节点

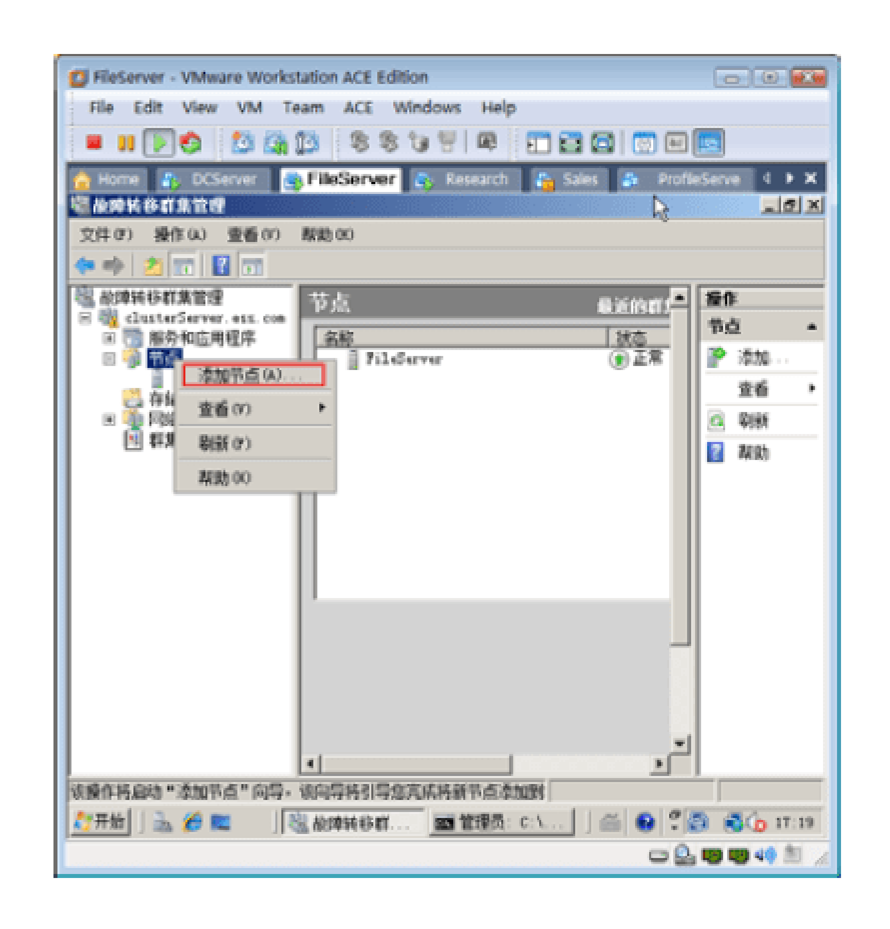


图 15-74 添加节点

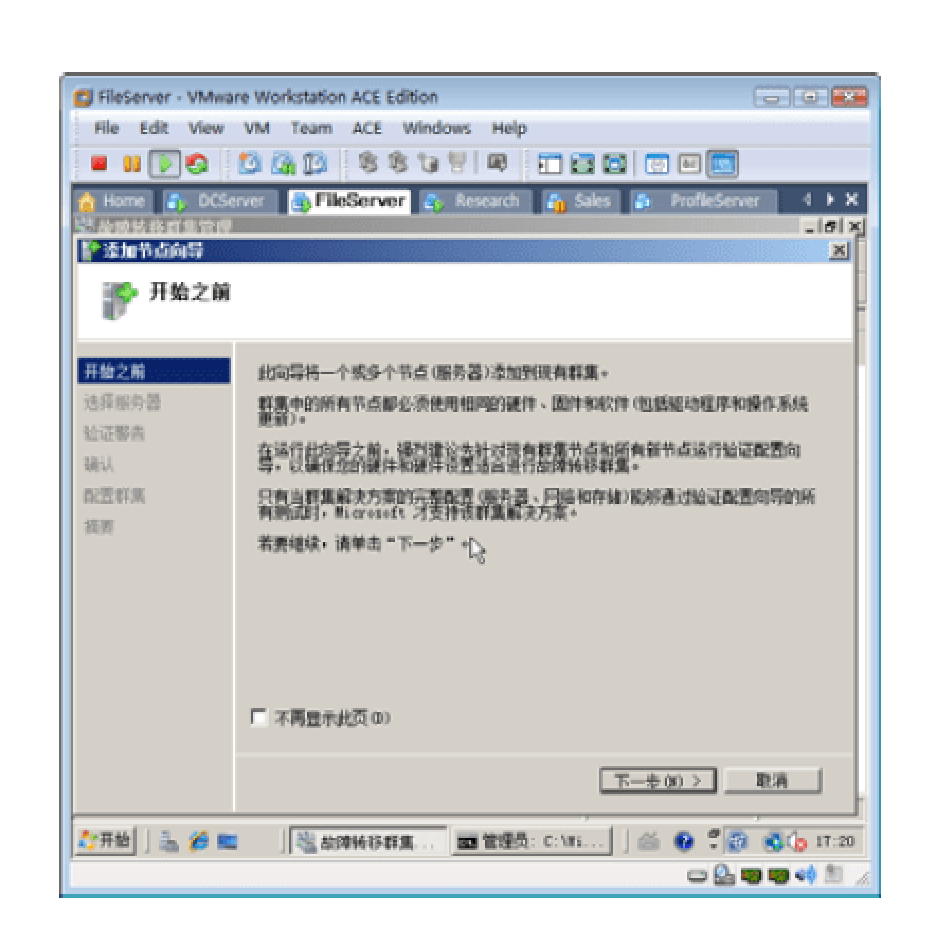


图 15-75 添加节点向导

⑦　如图 15-76 所示，在出现的“选择服务器”界面中，输入服务器名，单击“添加”按钮。

⑧　如图 15-77 所示，在出现的“确认”界面中，单击“下一步”按钮。

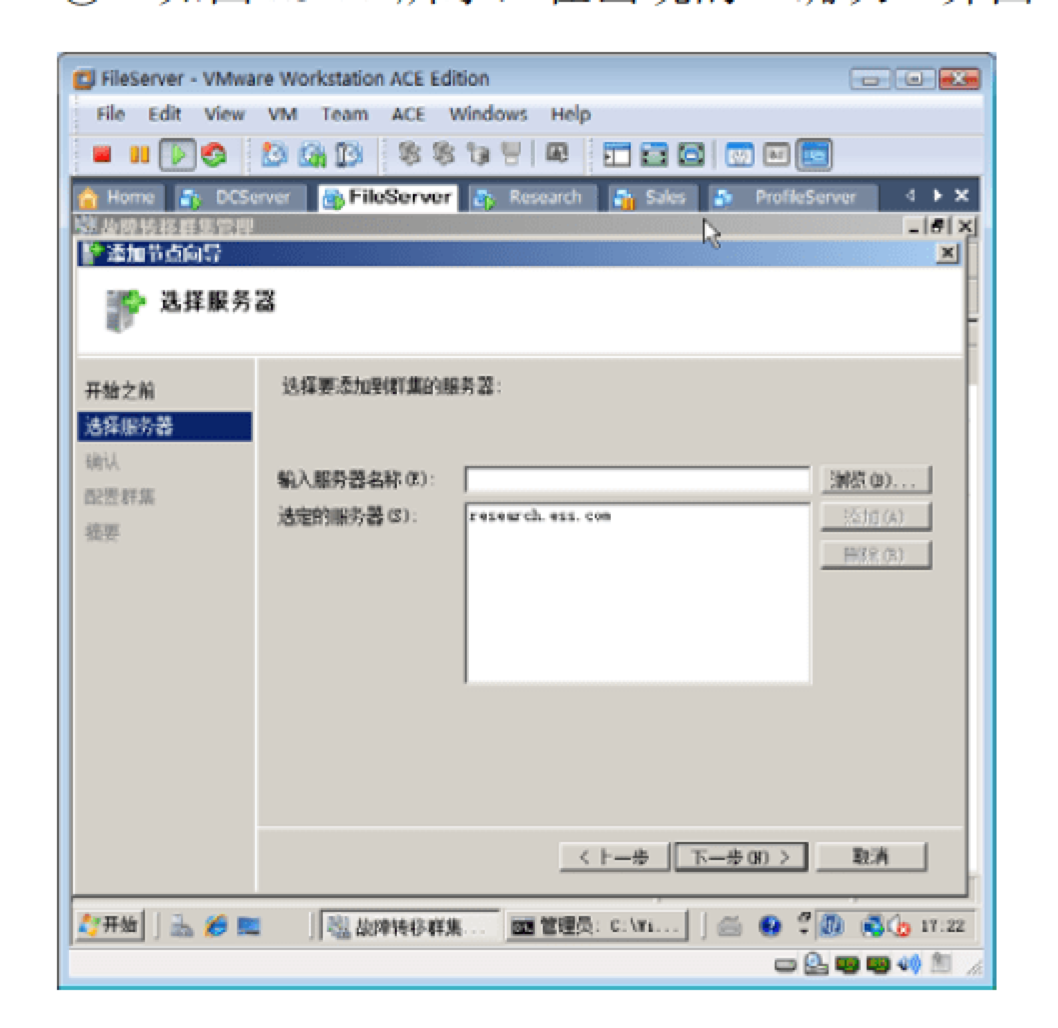


图 15-76　添加节点

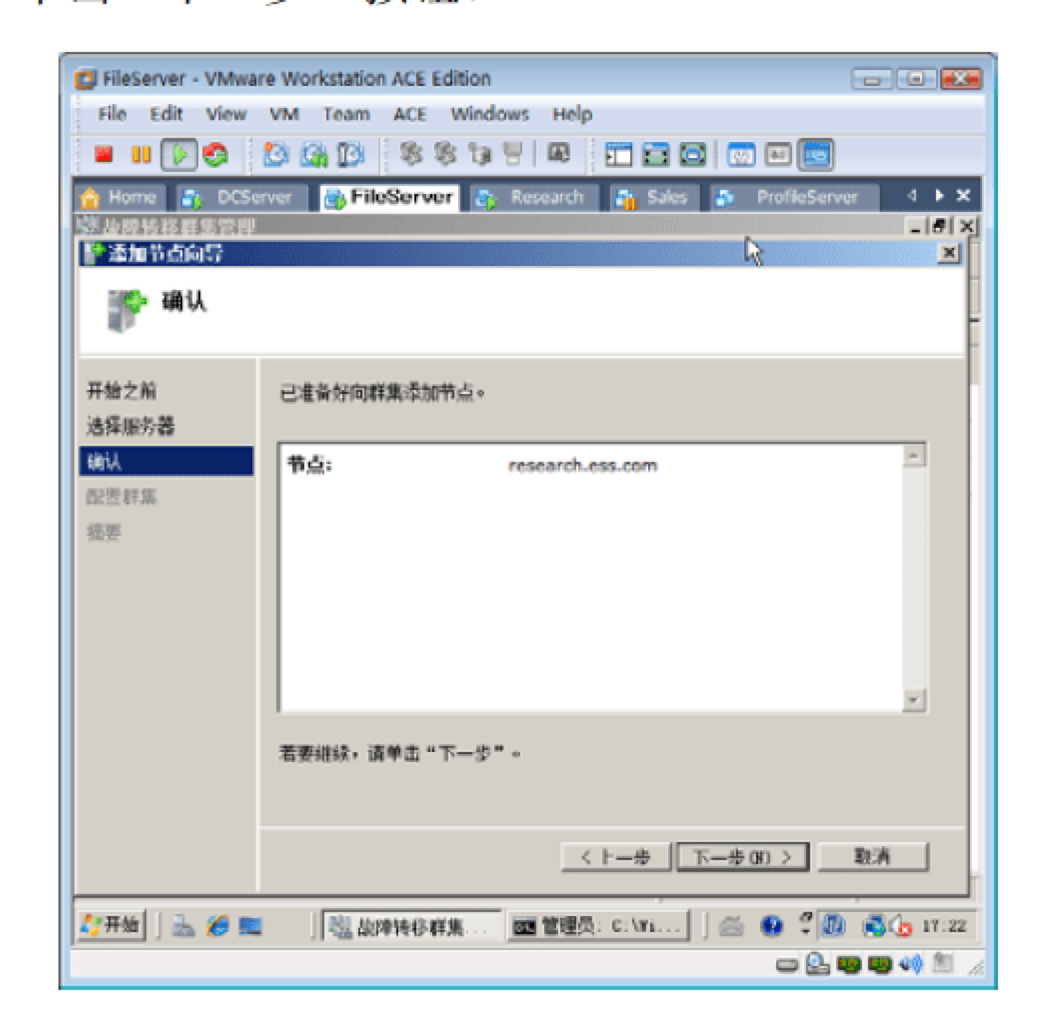


图 15-77　“确认”对话框

⑨　如图 15-78 所示，在“摘要”界面中，单击“完成”按钮。

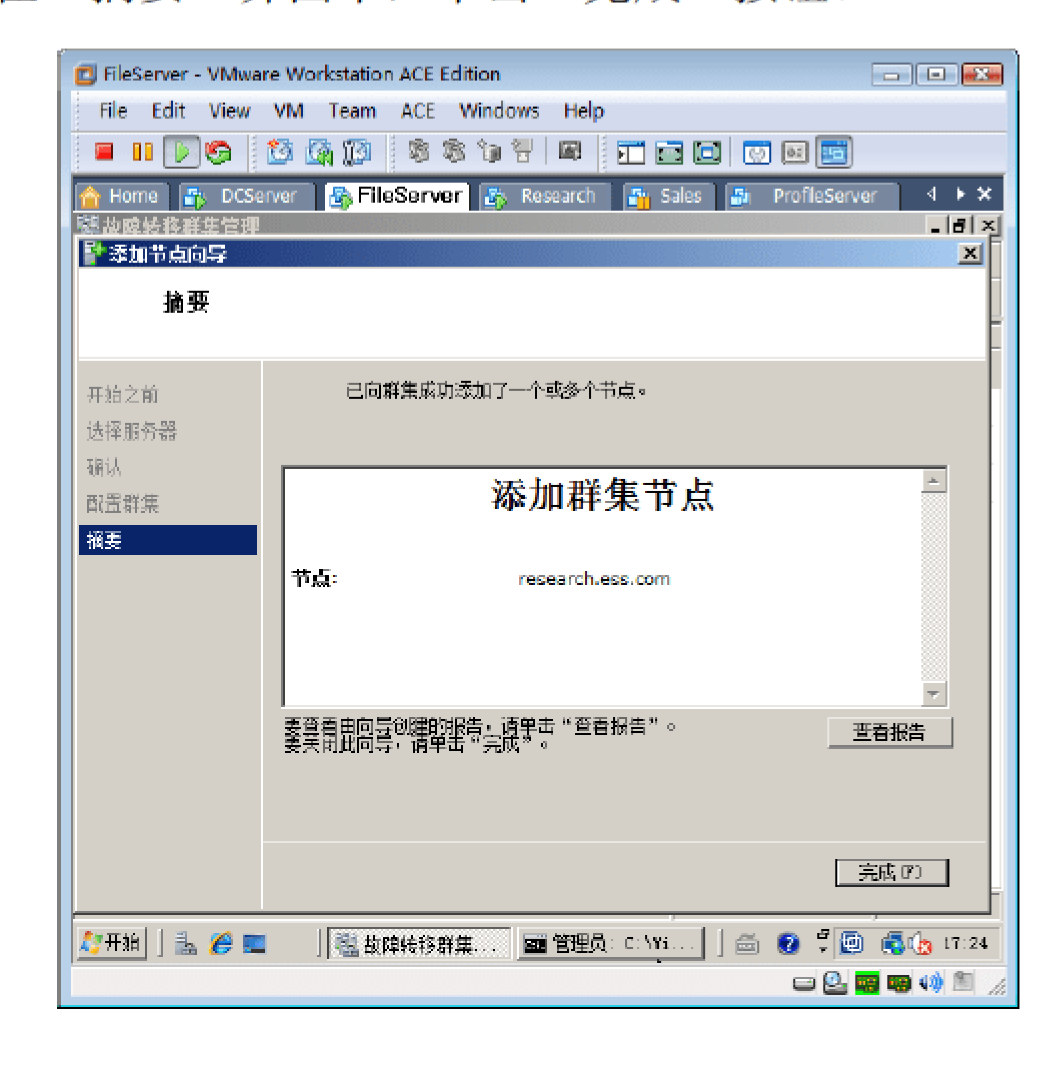


图 15-78　添加节点成功

15.6.7　确定仲裁磁盘

如图 15-79 所示，单击“存储”选项，可以看到 Q 磁盘为“仲裁中的见证磁盘”。

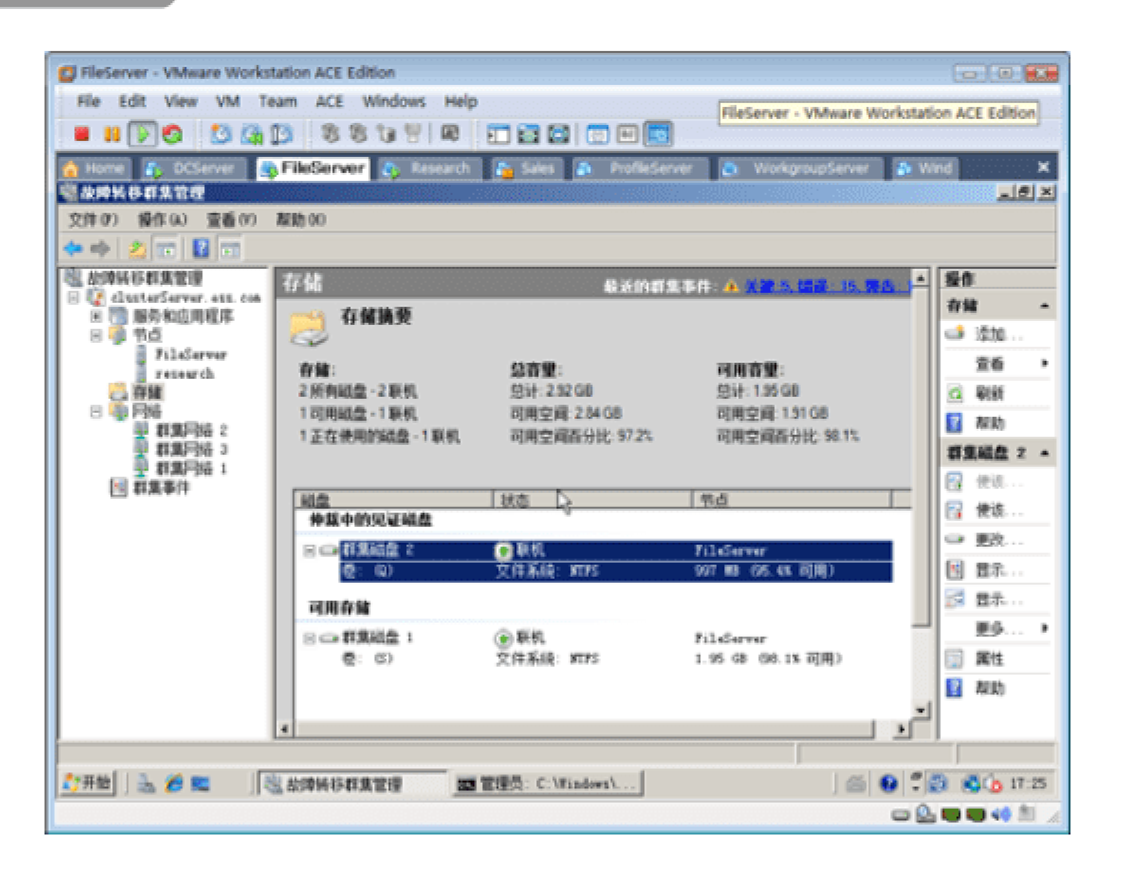


图 15-79　确定仲裁磁盘

15.7　配置文件服务器双节点群集

配置好 Windows Server 2008 的故障转移群集后，可以配置应用程序群集，如图 15-80 所示。以下将会在 FileServer 和 Research 节点安装文件服务角色。在群集环境中配置文件服务器群集，使用网络存储服务器 S 分区存储文件服务器共享文件夹。

文件服务器群集名称：ClusterServerFS。

文件服务器群集 IP 地址：10.7.10.10。

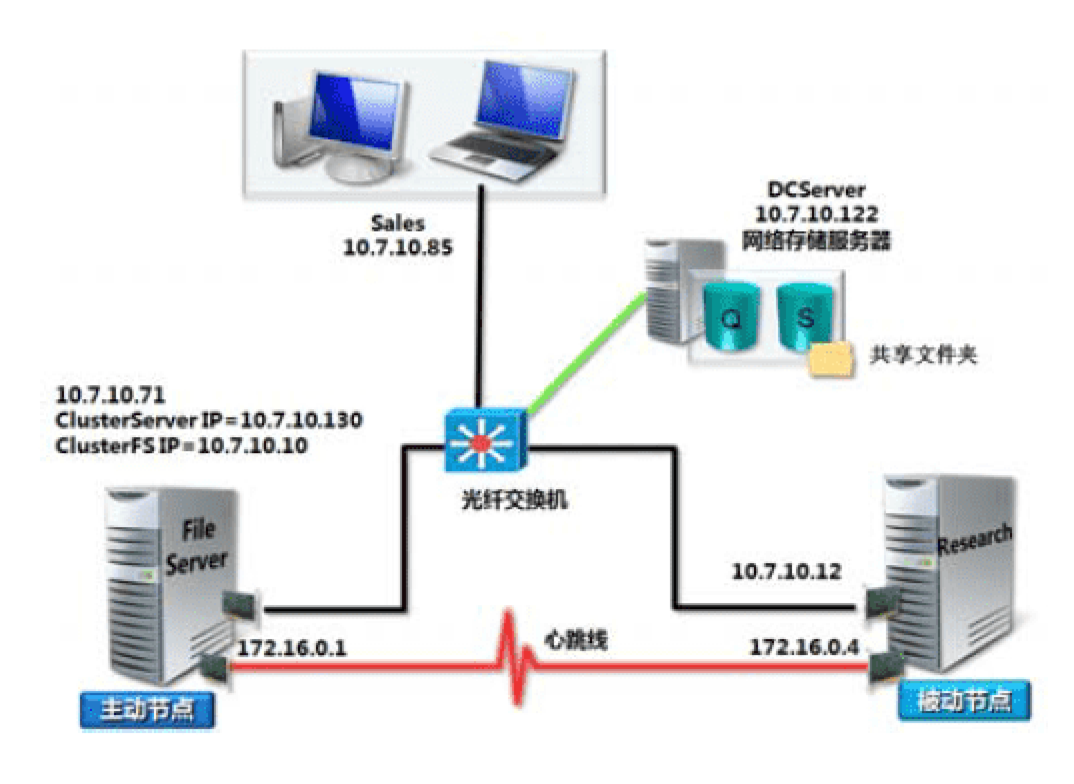


图 15-80　文件服务器群集

15.7.1　安装文件服务角色

在 FileServer 节点，安装文件服务角色。在 Research 节点，安装文件服务角色。

① 如图 15-81 所示，打开群集节点 FileServer 的服务器管理器，单击“添加角色”按钮。

② 如图 15-82 所示，在出现的“开始之前”界面中，单击“下一步”按钮。

③ 如图 15-83 所示，在出现的“选择服务器角色”界面中，选中“文件服务”复选框，单击“下一步”按钮。

④ 如图 15-84 所示，在出现的“文件服务”界面中，单击“下一步”按钮。

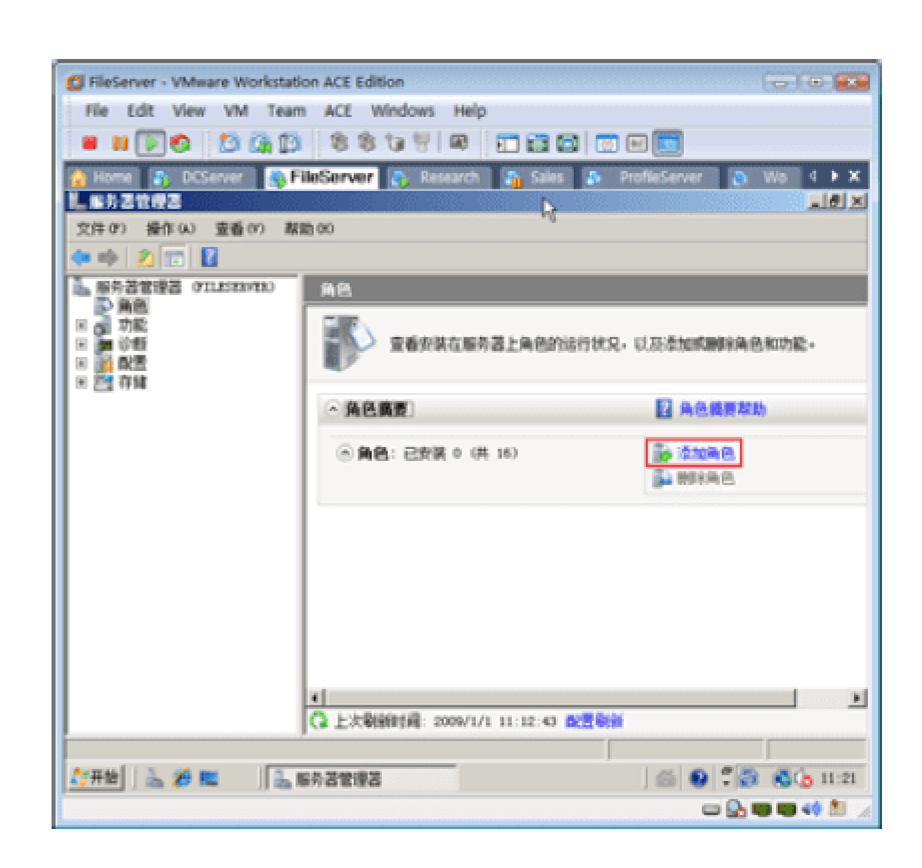


图 15-81　添加角色

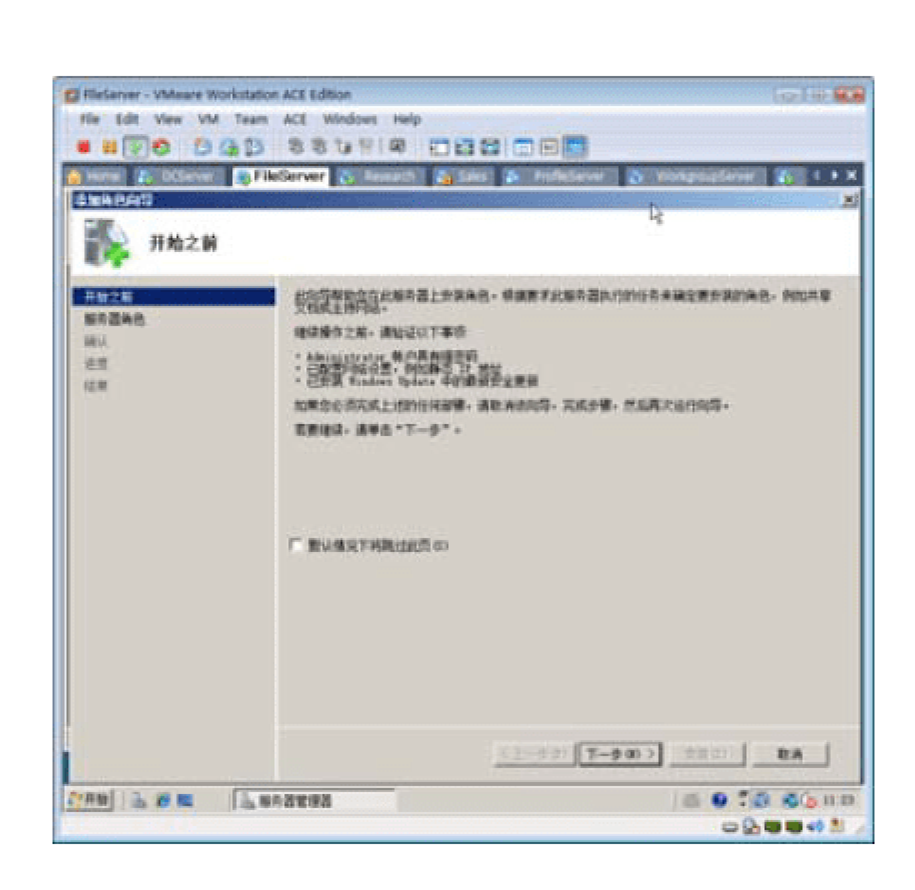


图 15-82　添加角色向导

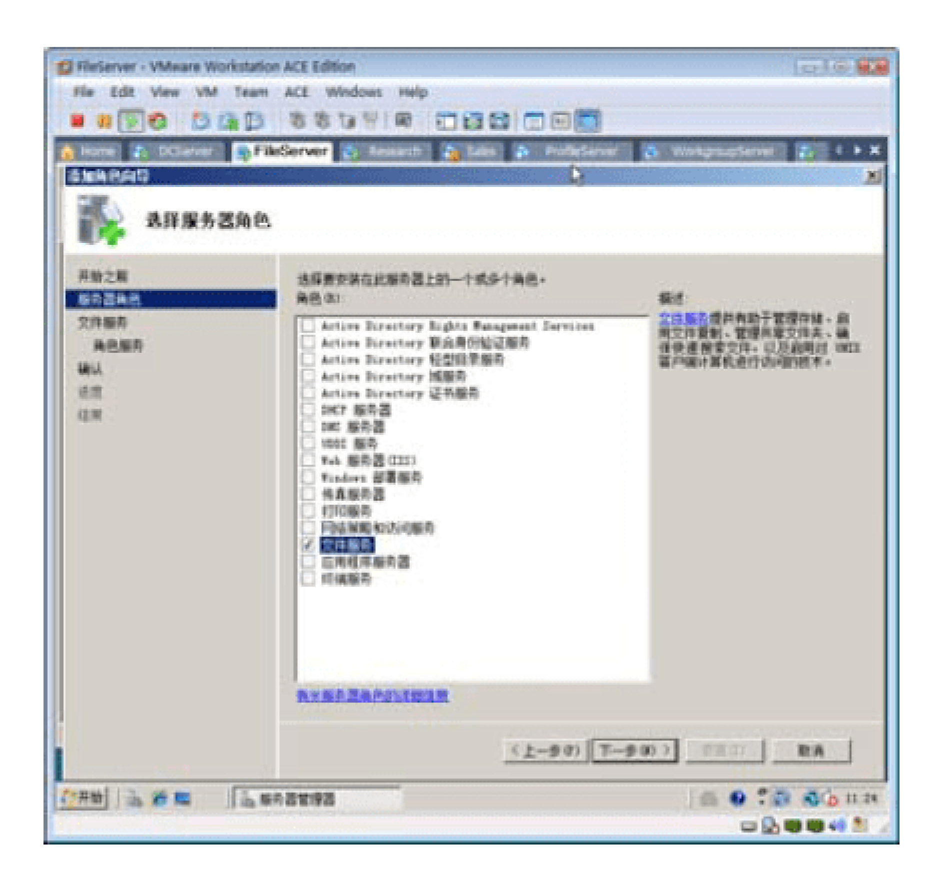


图 15-83　安装文件服务器角色

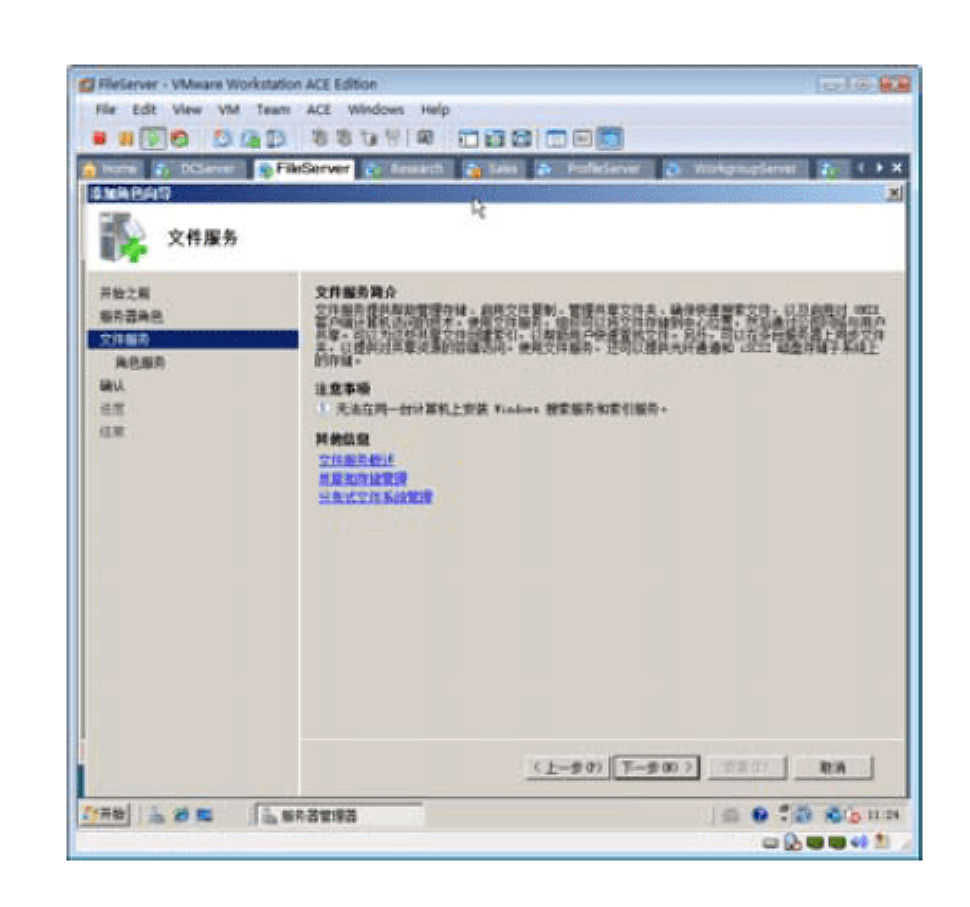


图 15-84　文件服务角色介绍

⑤　如图 15-85 所示，在出现的“选择角色服务”界面中，选中“文件服务器”复选框，单击“下一步”按钮。

⑥　如图 15-86 所示，在出现的“确认安装选择”界面中，单击“安装”按钮。

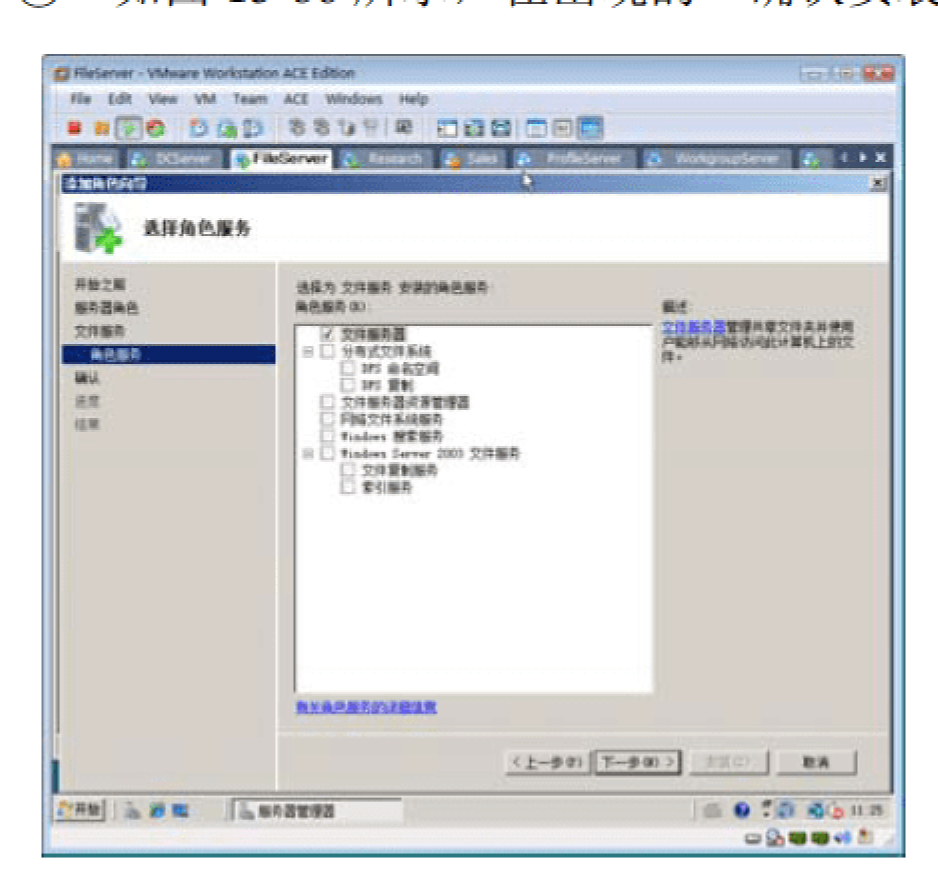


图 15-85　选择角色服务

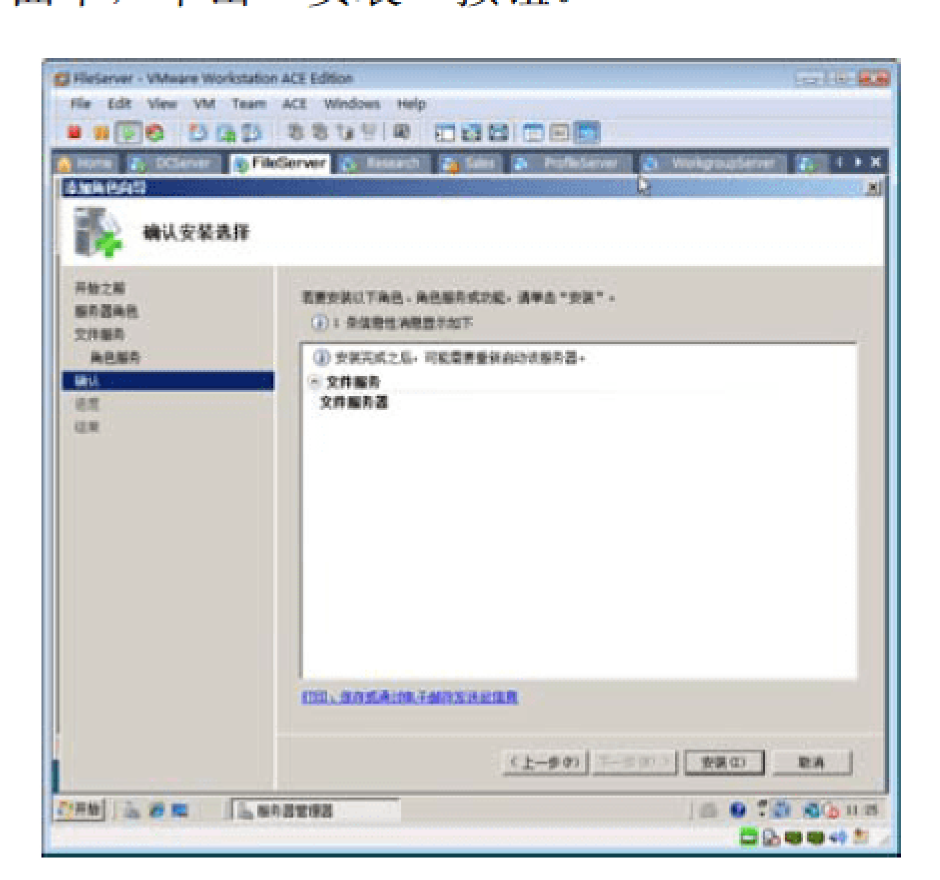


图 15-86　确认安装选择

⑦ 完成文件服务器安装。

⑧ 按照在 FileServer 上安装文件服务器角色相同的步骤，在 Research 服务器上安装文件服务器角色。

15.7.2 配置文件服务群集

在 Windows 群集配置好后，再配置文件服务器群集。

① 如图 15-87 所示，右击“服务和应用程序”，在弹出的快捷菜单中选择“配置服务或应用程序”命令。

② 如图 15-88 所示，在出现的向导对话框中，单击“下一步”按钮。

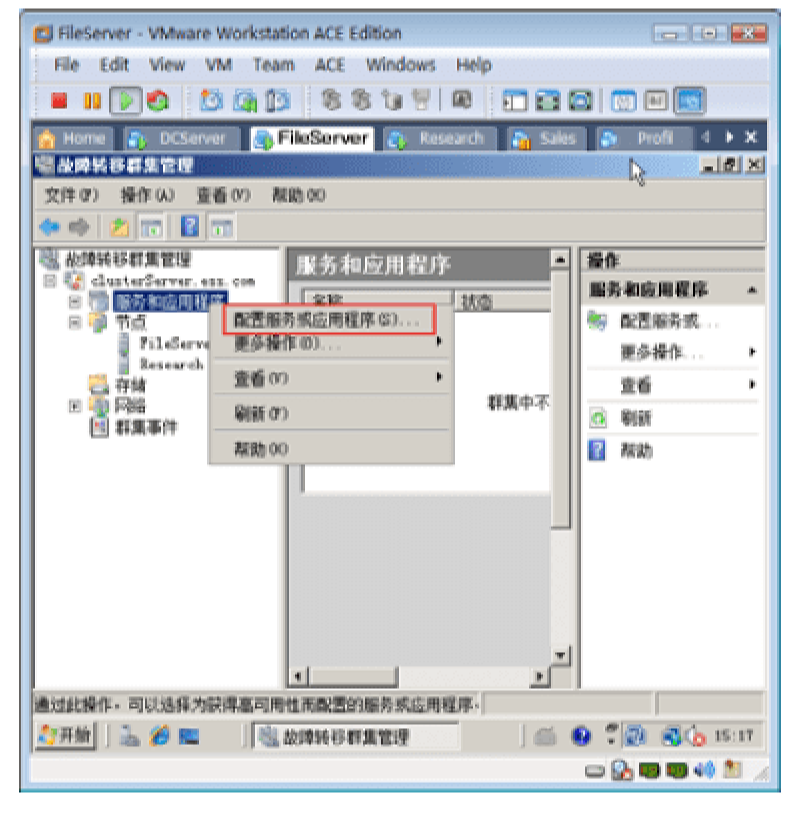


图 15-87 配置服务器或应用程序

图 15-88 配置向导

③ 如图 15-89 所示，在“选择服务或应用程序”界面中，选中“文件服务器”选项，单击“下一步”按钮。

④ 如图 15-90 所示，在“客户端访问点”界面中，输入名称 clusterFS 和群集地址 10.7.10.10，单击“下一步”按钮。

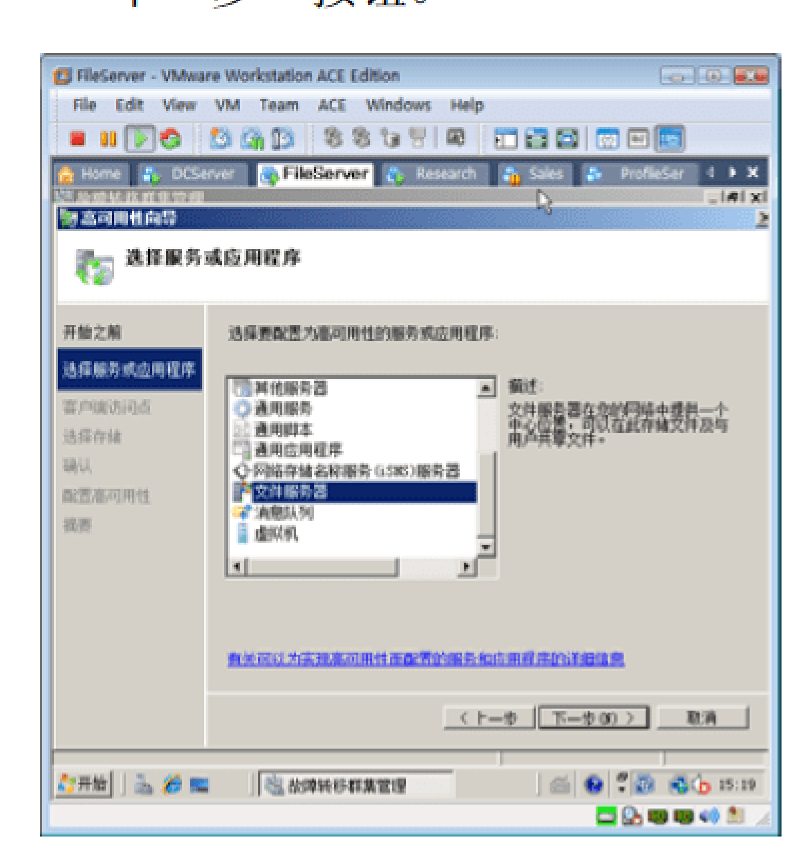




图 15-89 选择文件服务器

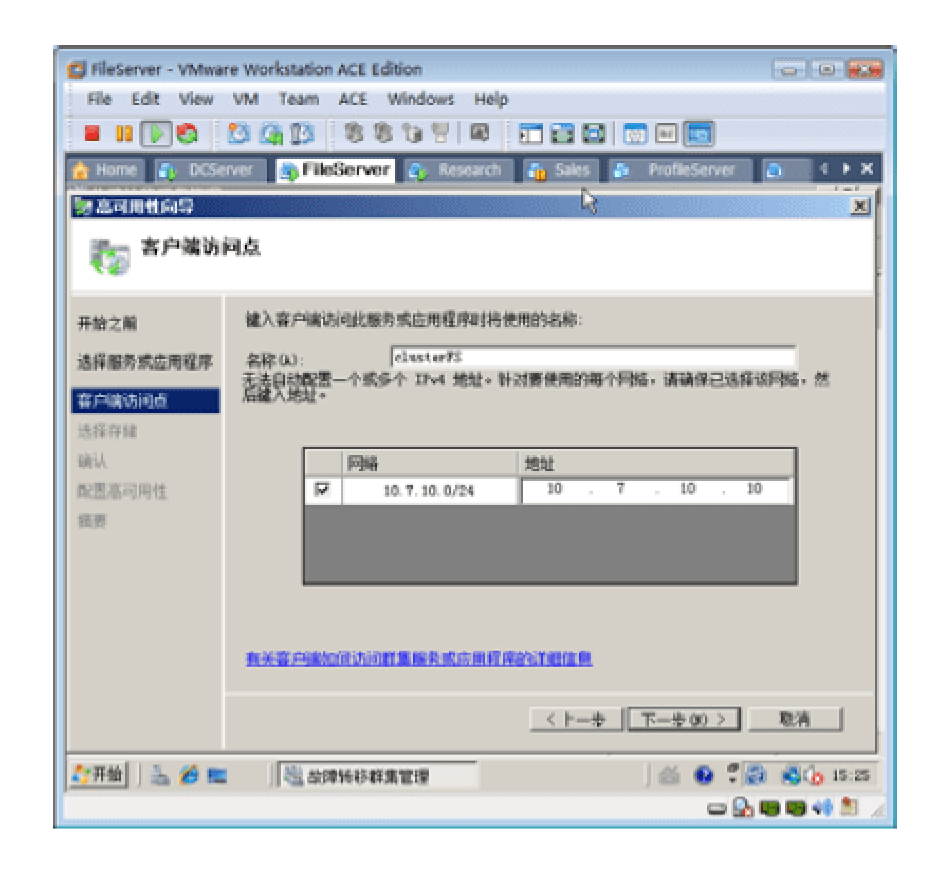


图 15-90 指定 IP 地址和名称

⑤ 如图 15-91 所示，在“选择存储”界面中，选中“群集磁盘 1”，单击“下一步”按钮。

⑥ 如图 15-92 所示，在“确认”界面中，单击“下一步”按钮。

⑦　如图 15-93 所示，出现“配置高可用性”界面。

⑧　如图 15-94 所示，在出现的“摘要”界面中，单击“完成”按钮。

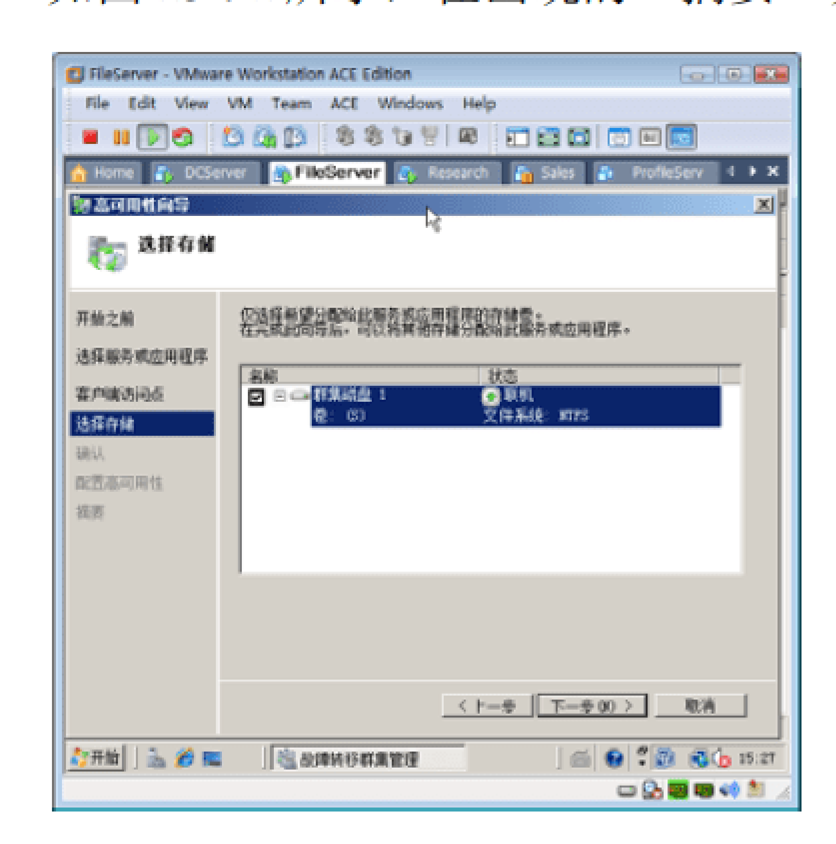


图 15-91　指定群集磁盘

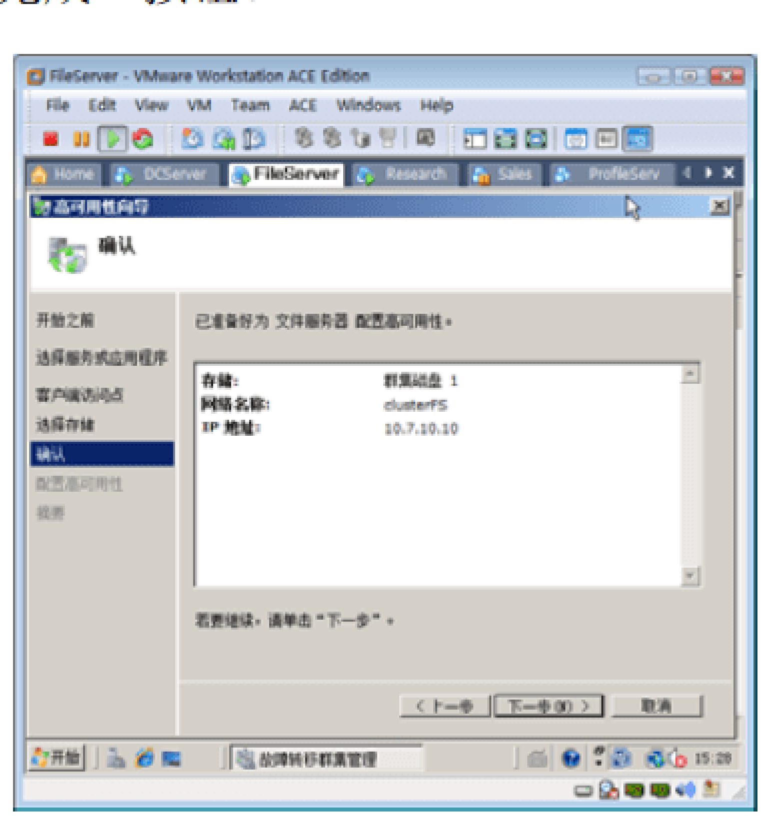


图 15-92　“确认”对话框

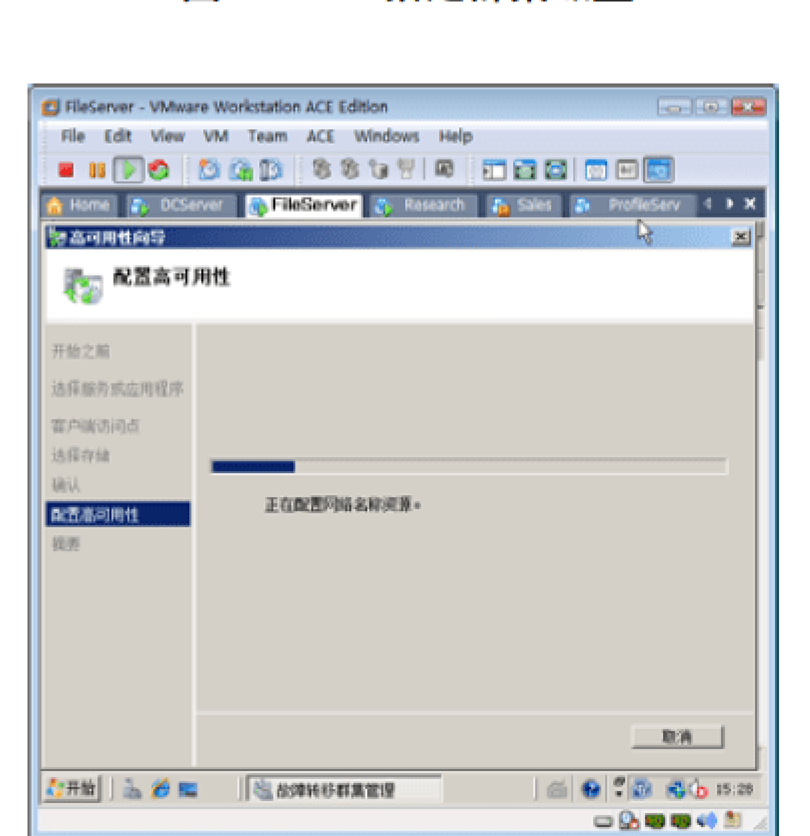


图 15-93　配置高可用性

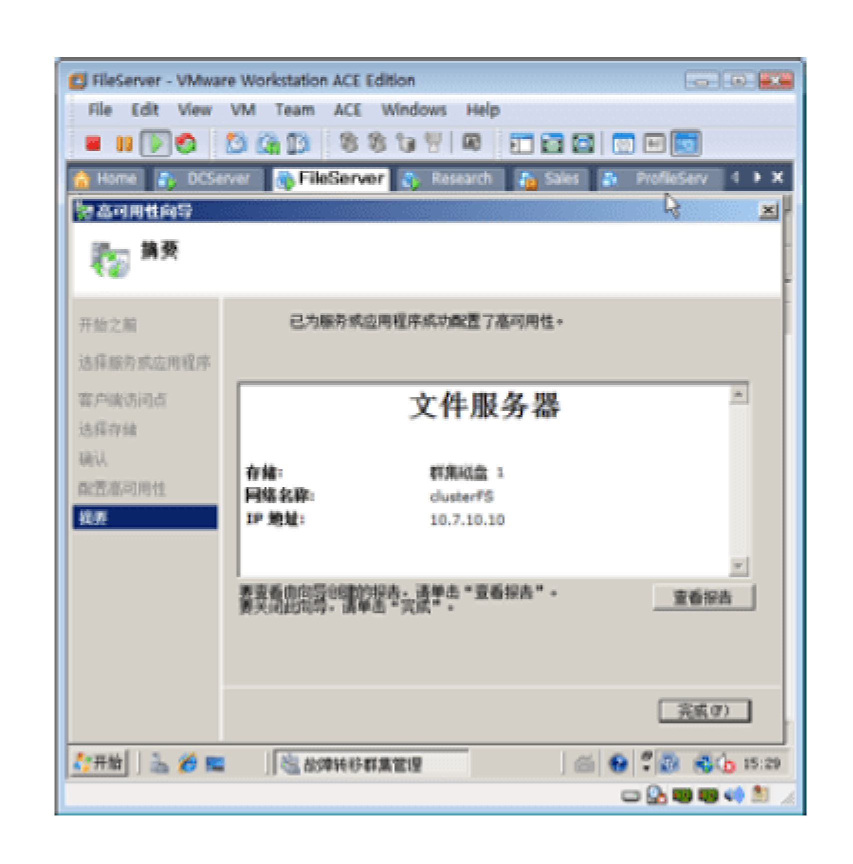


图 15-94　完成文件服务器群集

⑨　如图 15-95 所示，可以看到 clusterFS 文件服务器首选的节点以及当前的所有者，能看到文件服务器的 IP 地址为 10.7.10.10。

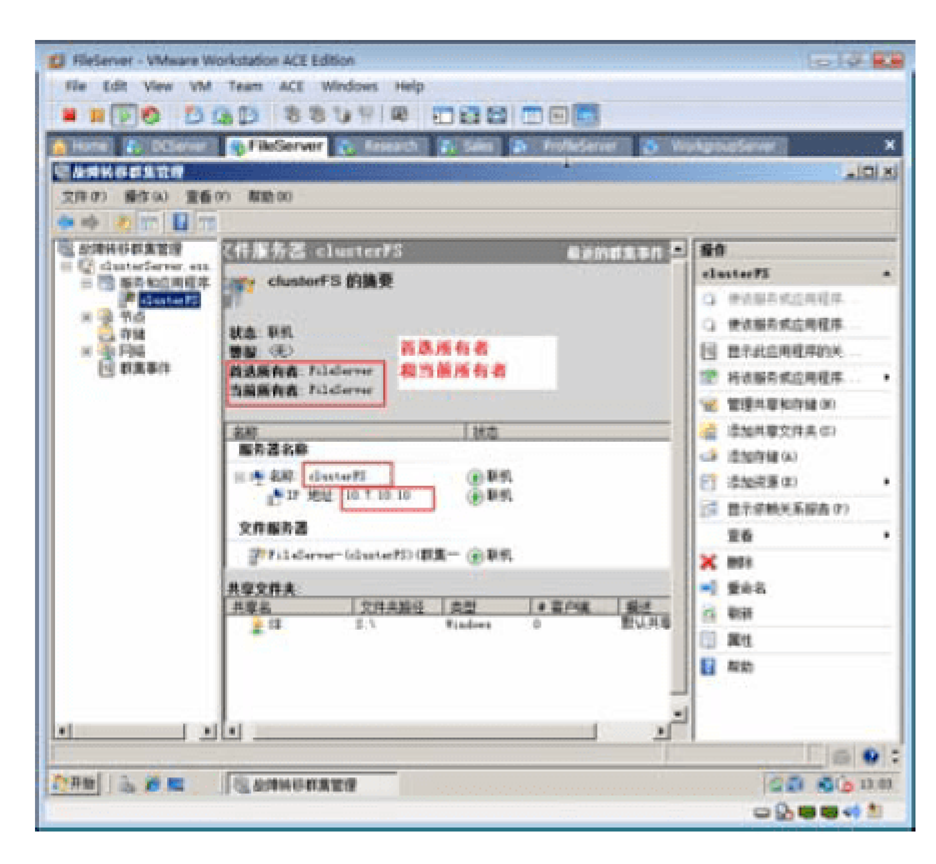


图 15-95　文件服务器群集

15.7.3 添加共享文件夹

在群集的文件服务器 clusterFS 添加共享文件夹 shareData。

① 如图 15-96 所示，在 FileServer 服务器上，单击“添加共享文件夹”按钮。

② 如图 15-97 所示，在出现的“共享文件夹位置”界面中，单击“浏览”按钮。

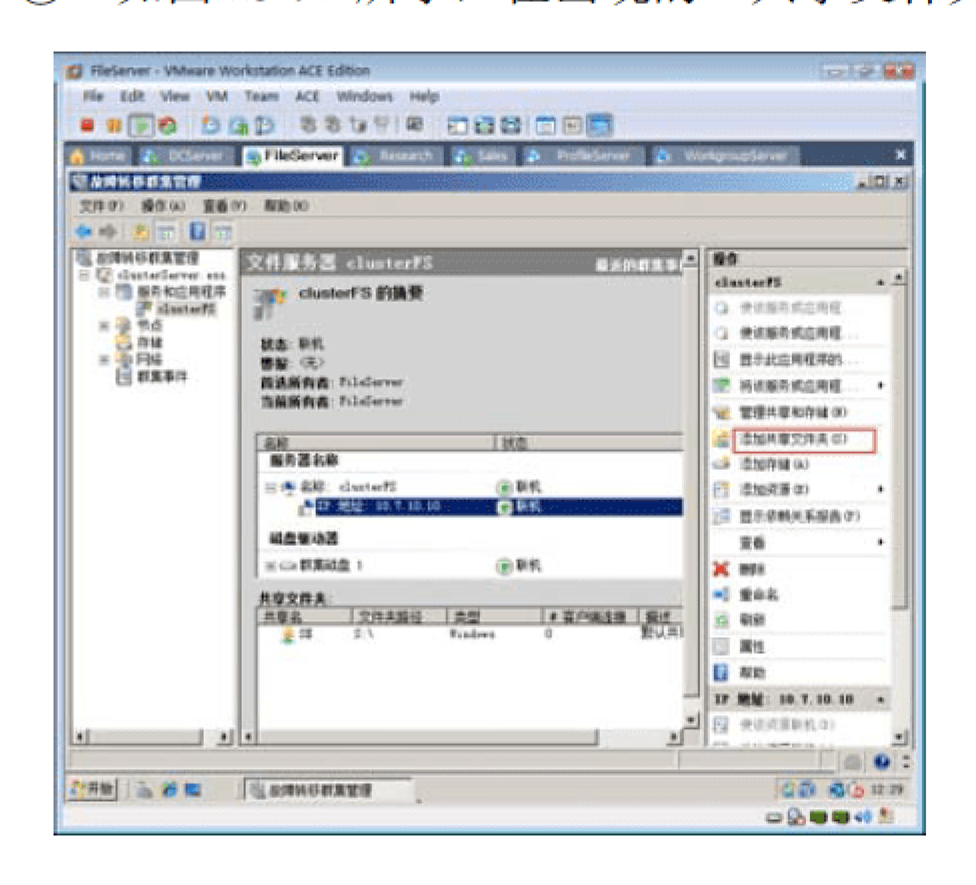


图 15-96 添加共享文件夹

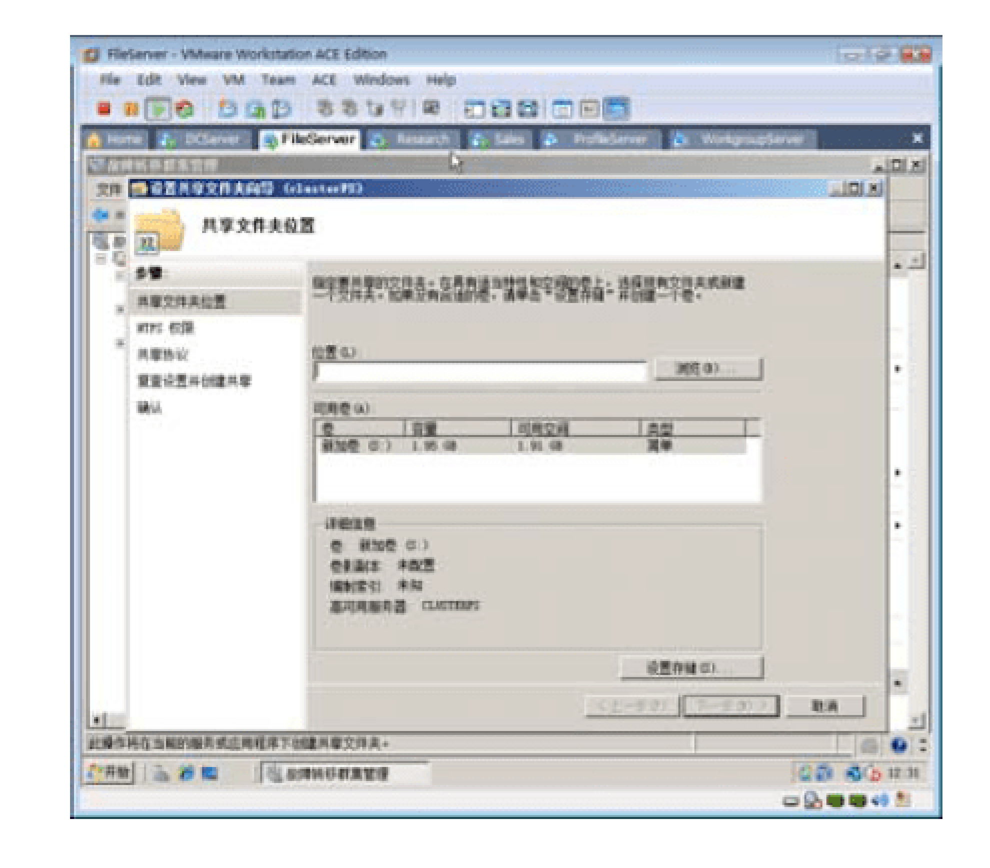


图 15-97 浏览文件夹

③ 如图 15-98 所示，在出现的“浏览文件夹”对话框中，选中 S$，单击“新建文件夹”按钮，输入 shareData，单击“确定”按钮。

④ 如图 15-99 所示，在“共享文件夹位置”对话框中，单击“下一步”按钮。

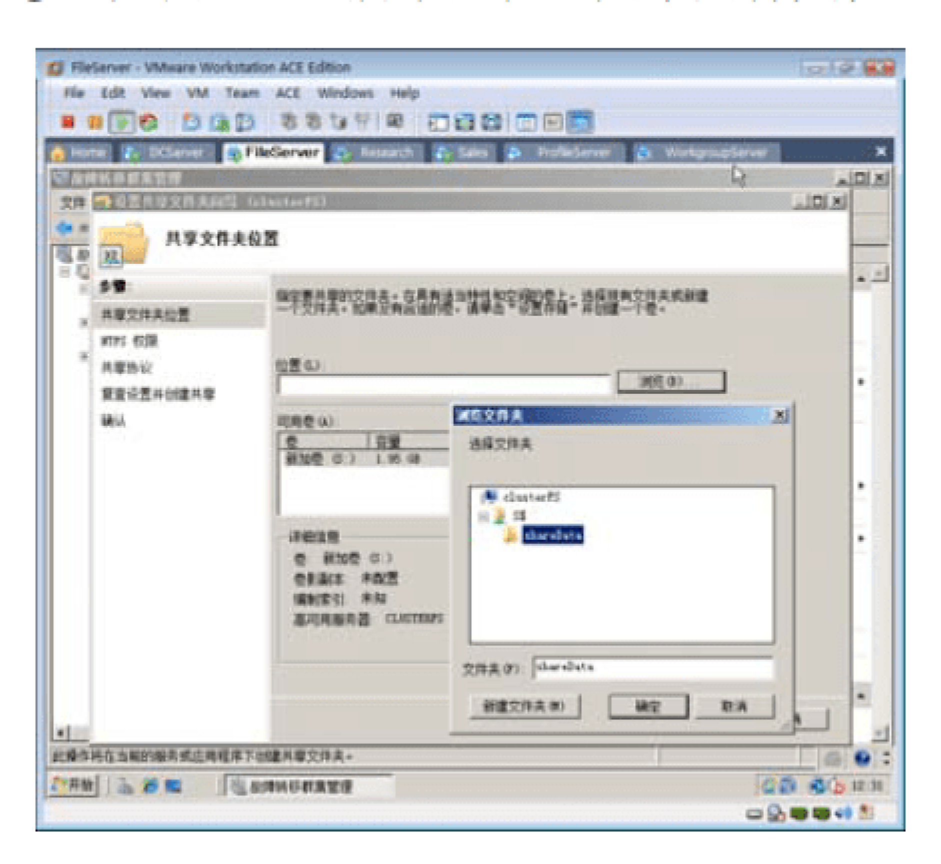


图 15-98 创建文件

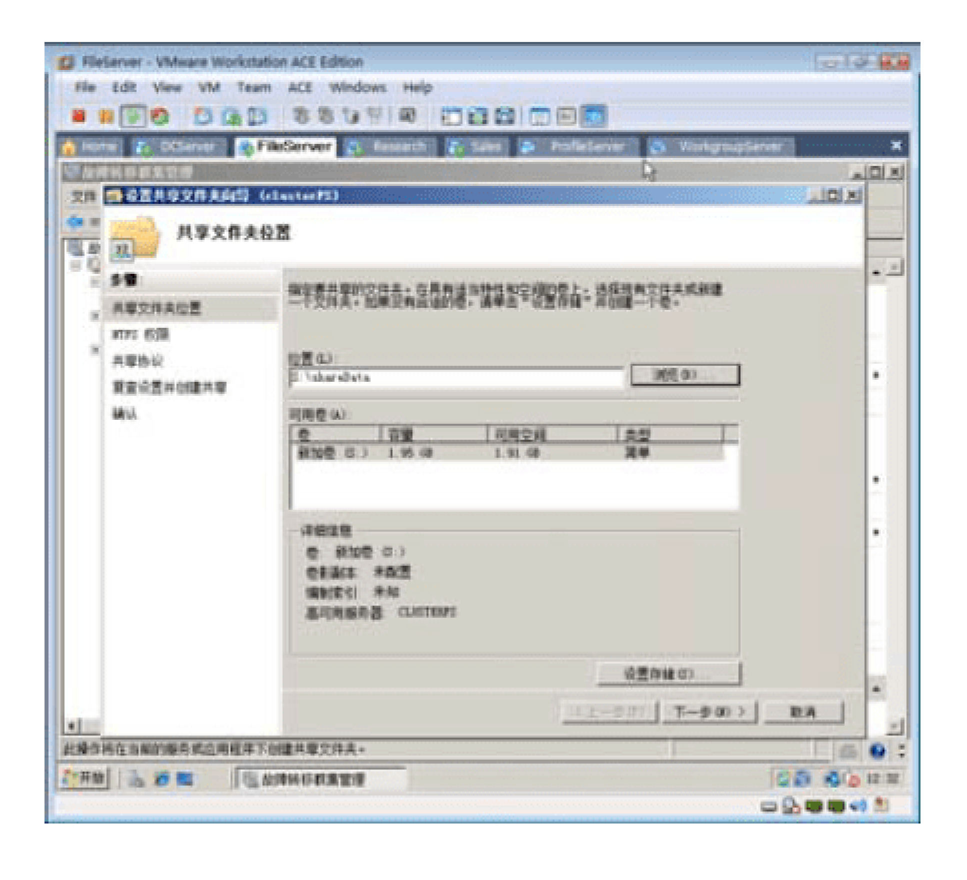


图 15-99 确认共享目录

⑤ 如图 15-100 所示，在“NTFS 权限”界面中，选中“否，不更改 NTFS 权限”单选按钮，单击“下一步”按钮。

⑥ 如图 15-101 所示，在“共享协议”界面中，选中 SMB 复选框，共享名输入 shareData，单击“下一步”按钮。

⑦ 如图 15-102 所示，在“SMB 设置”界面中，单击“下一步”按钮。

⑧ 如图 15-103 所示，在“SMB 权限”界面中，选中“Administrator 具有完全控制权限，所有其他

用户和组具有读写访问权限”单选按钮。

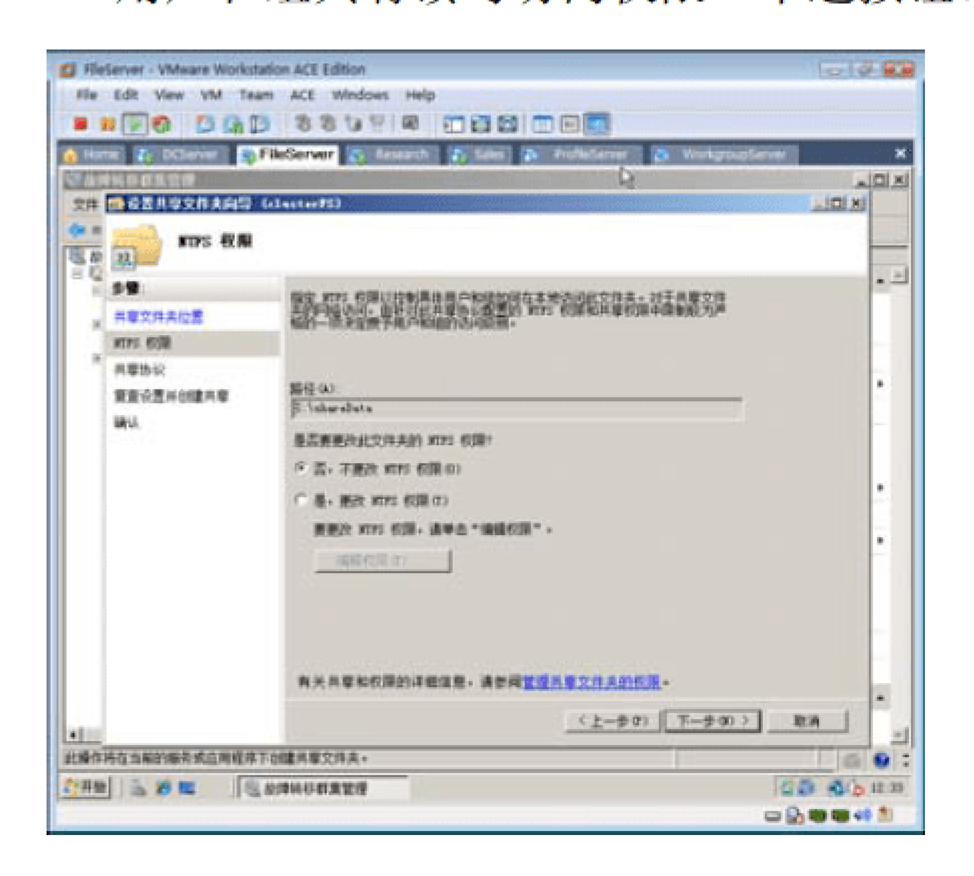


图 15-100　不更改 NTFS 权限

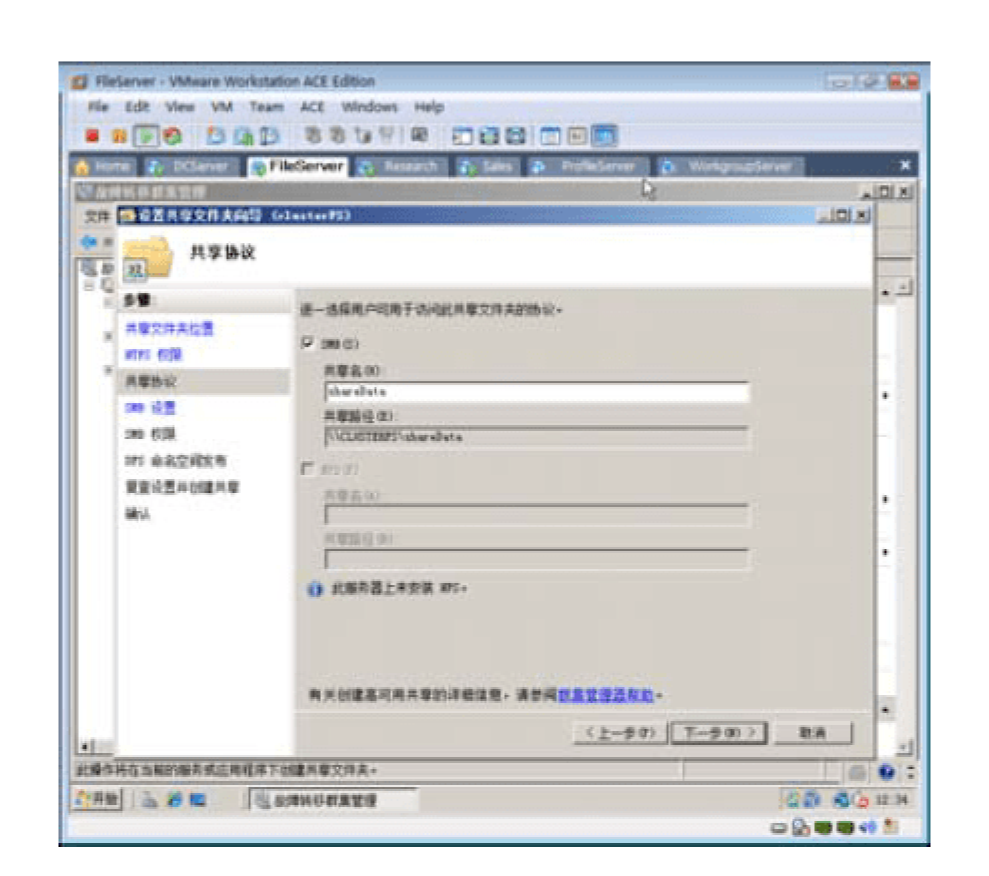


图 15-101　输入共享名

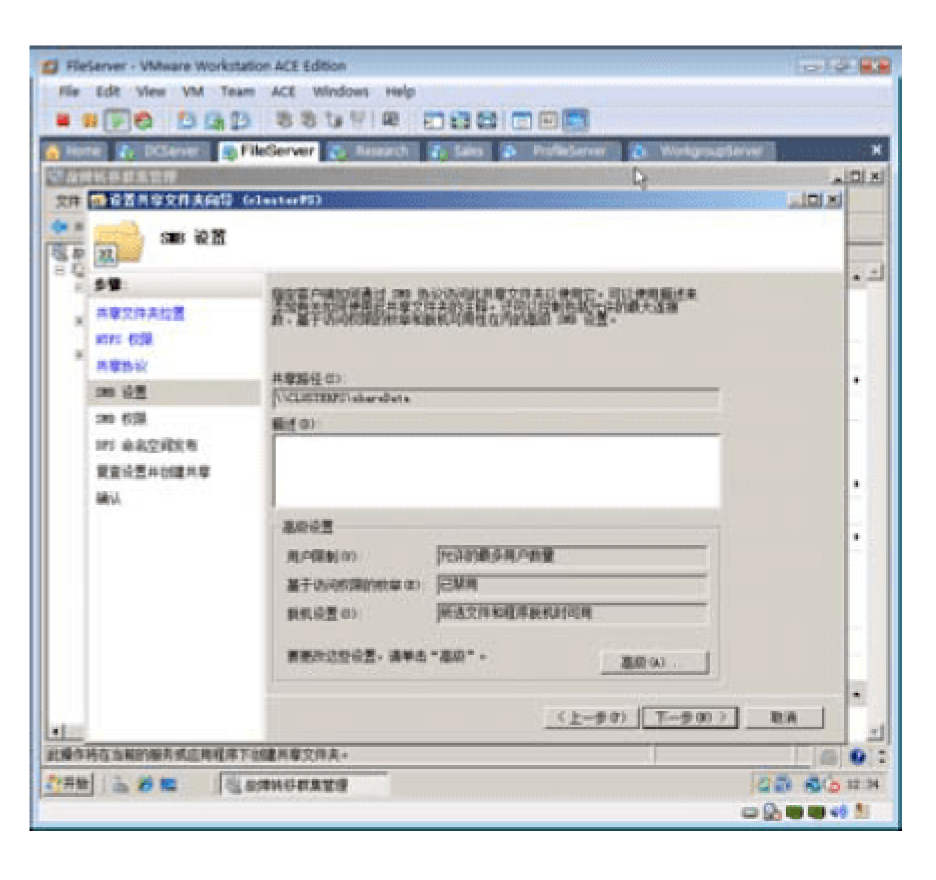


图 15-102　设置 SMB

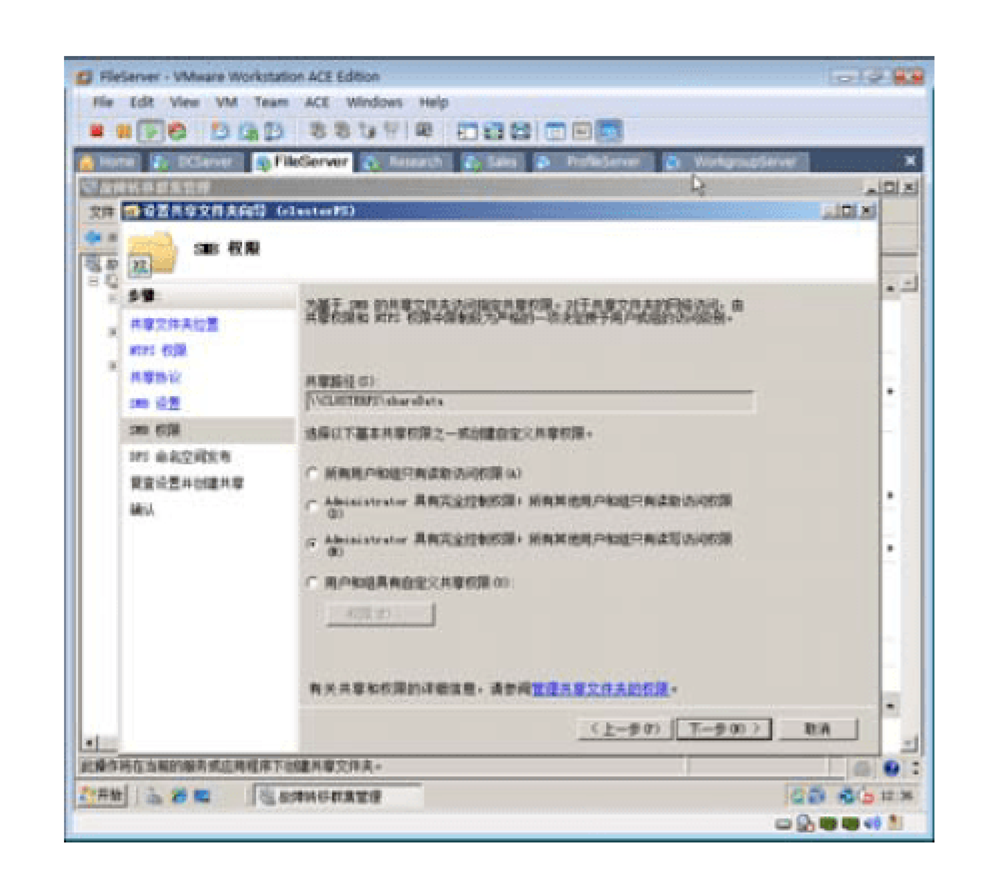


图 15-103　设置 SMB 权限

⑨　如图 15-104 所示，在“DFS 命名空间发布”界面中，单击“下一步”按钮。

⑩　如图 15-105 所示，在出现的“复查设置并创建共享”界面中，单击“创建”按钮。

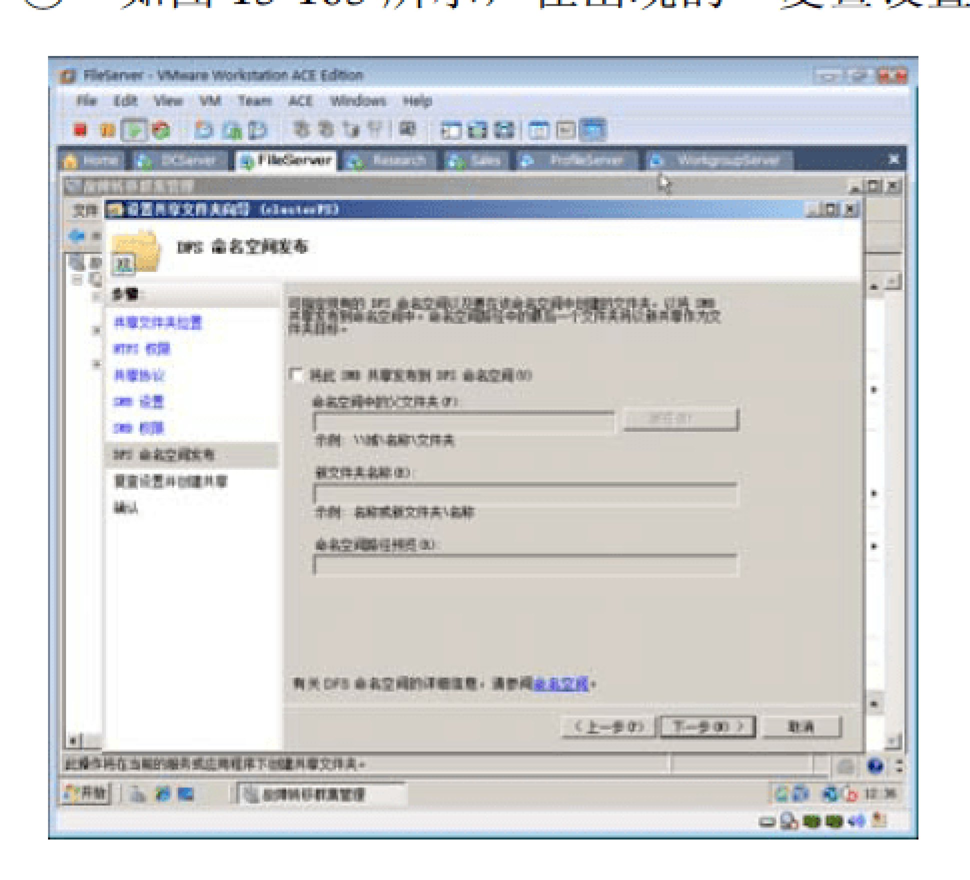


图 15-104　DFS 命名空间发布

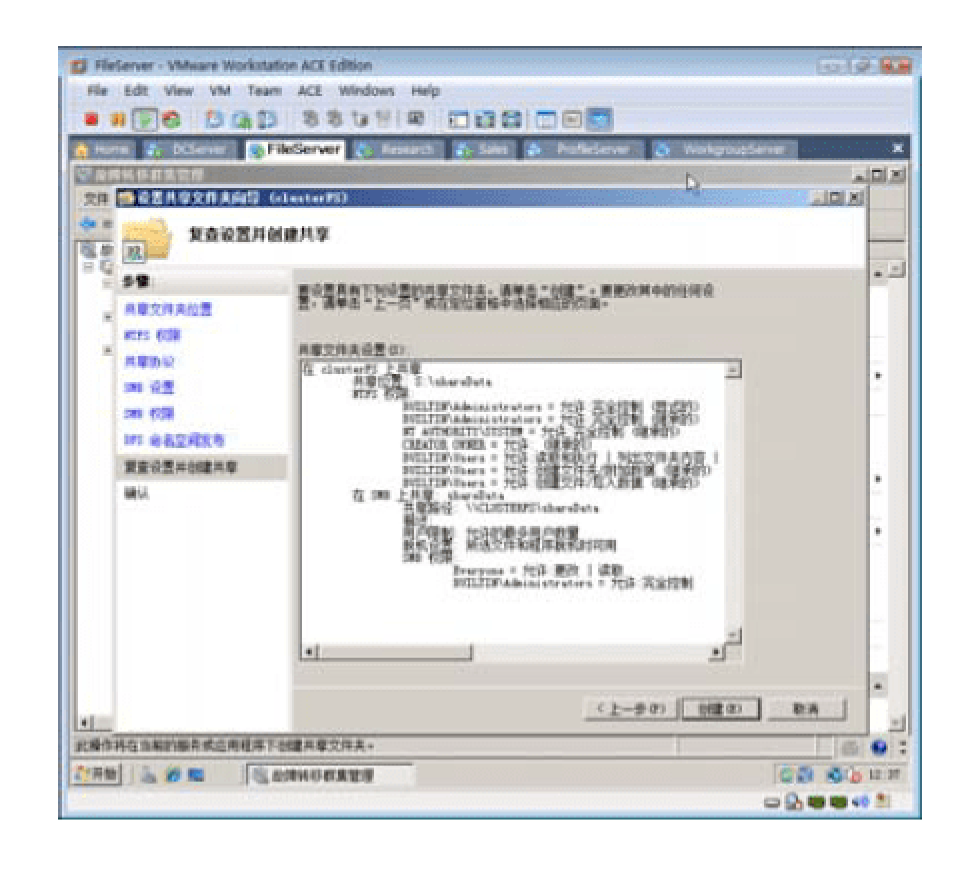


图 15-105　复查设置

⑪ 如图 15-106 所示，在“确认”界面中，单击“完成”按钮。

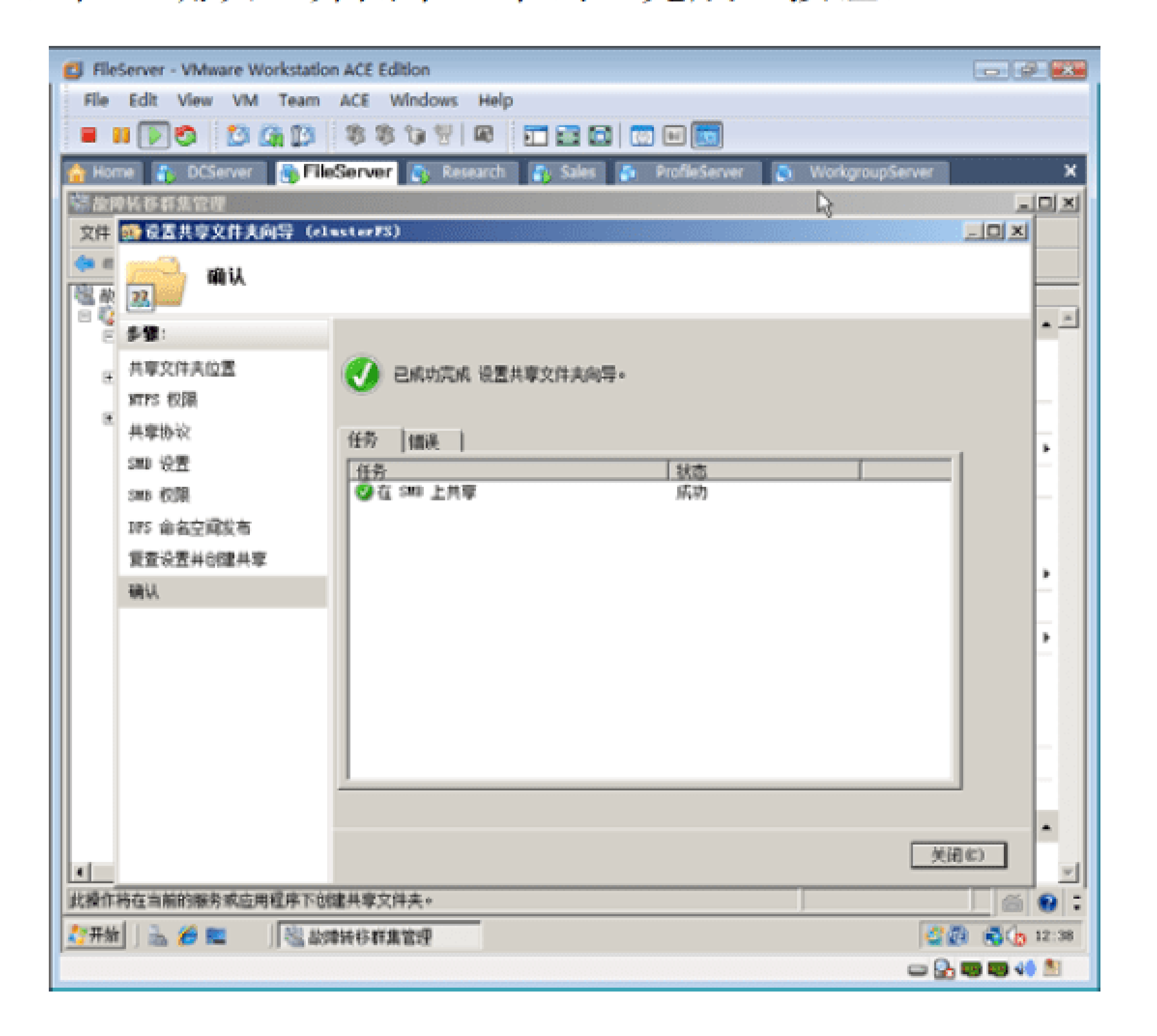


图 15-106　完成共享文件夹向导

15.7.4　移动节点

① 如图 15-107 所示，右击 clusterFS，在弹出的快捷菜单中选择“将该服务或应用程序移动到另一个节点”→“移动到节点 Research”命令。

② 如图 15-108 所示，在出现的“请确认操作”对话框中，单击“将 clusterFS 移动到 Research”按钮。

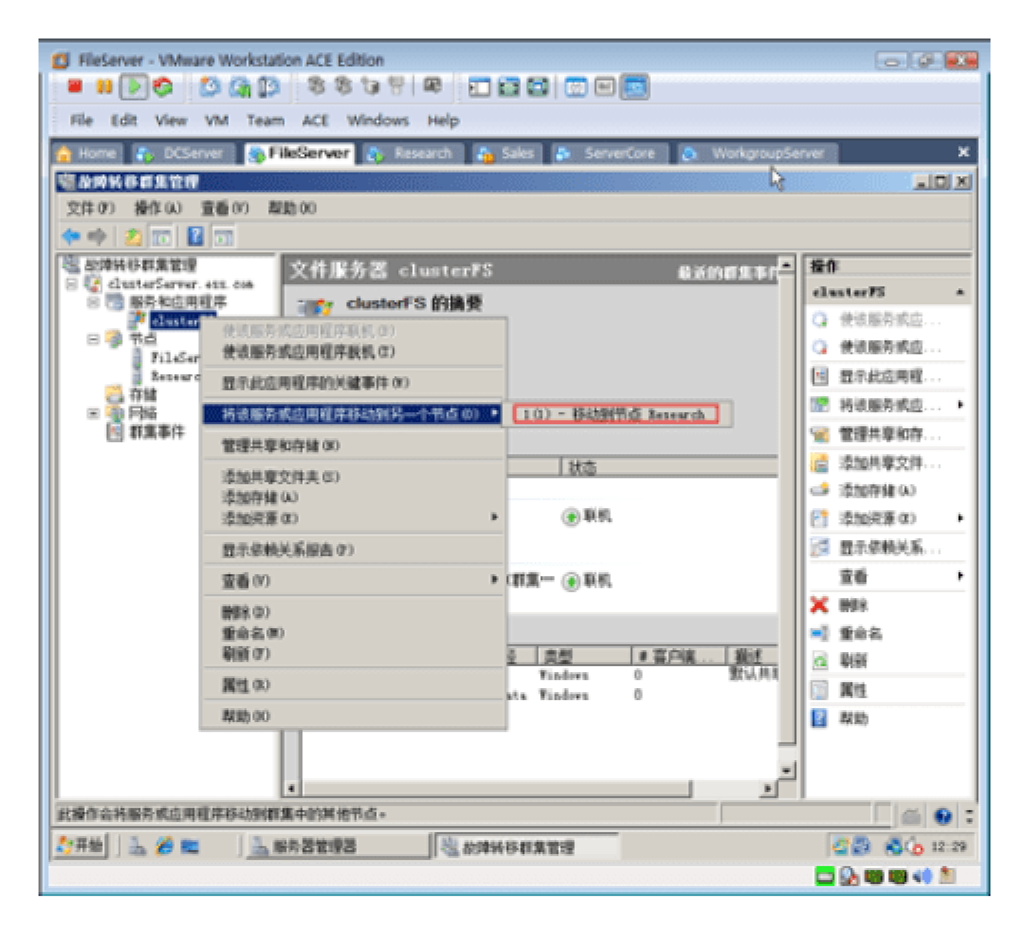


图 15-107　移动群集

图 15-108　确认移动

③ 如图 15-109 所示，可以看到在移动过程中资源处于脱机状态。

④ 如图 15-110 所示，启动完成后可以看到当前所有者是 Research 节点。

⑤ 按照以上步骤将 clusterFS 移动到 FileServer。

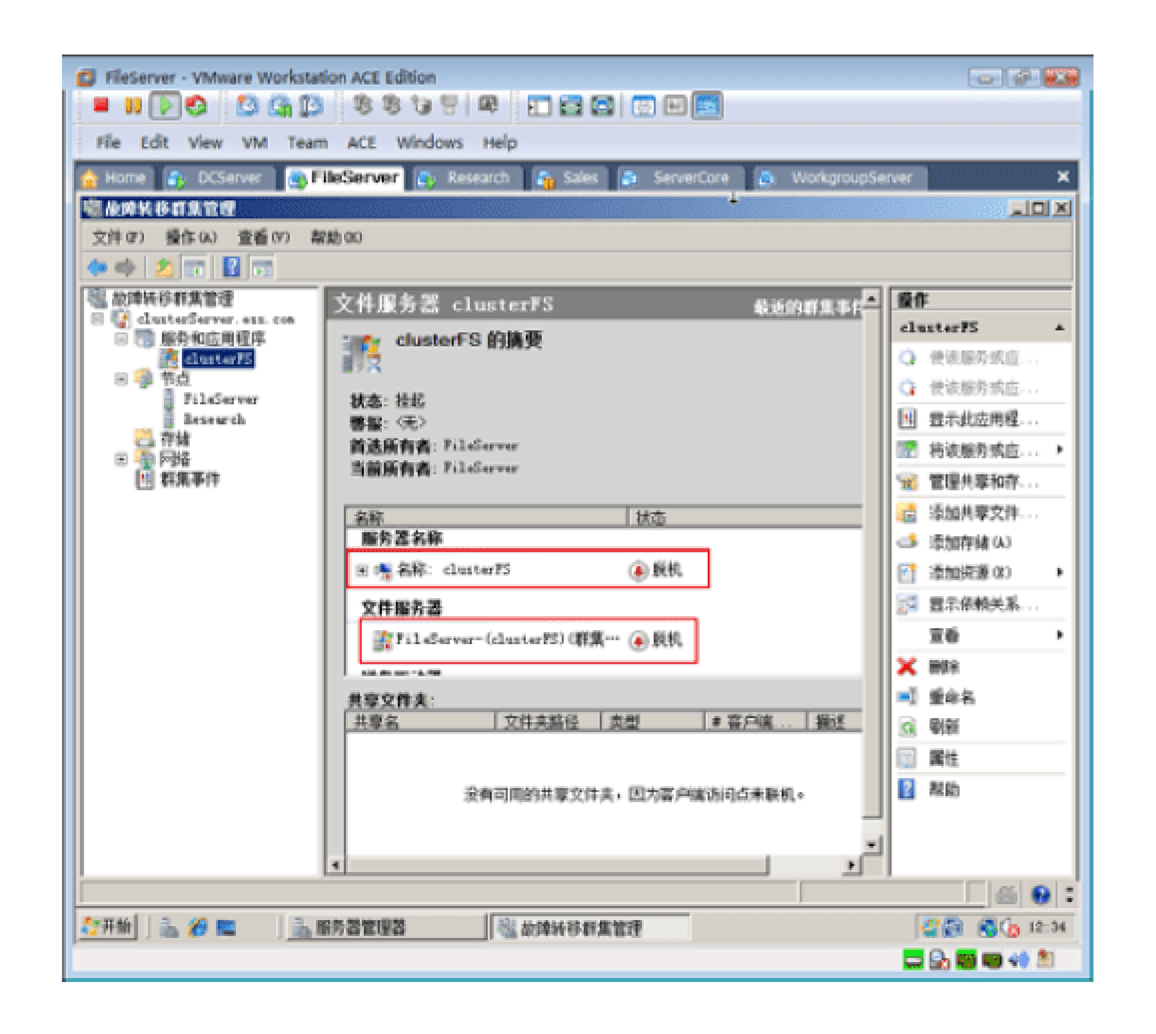


图 15-109　移动过程

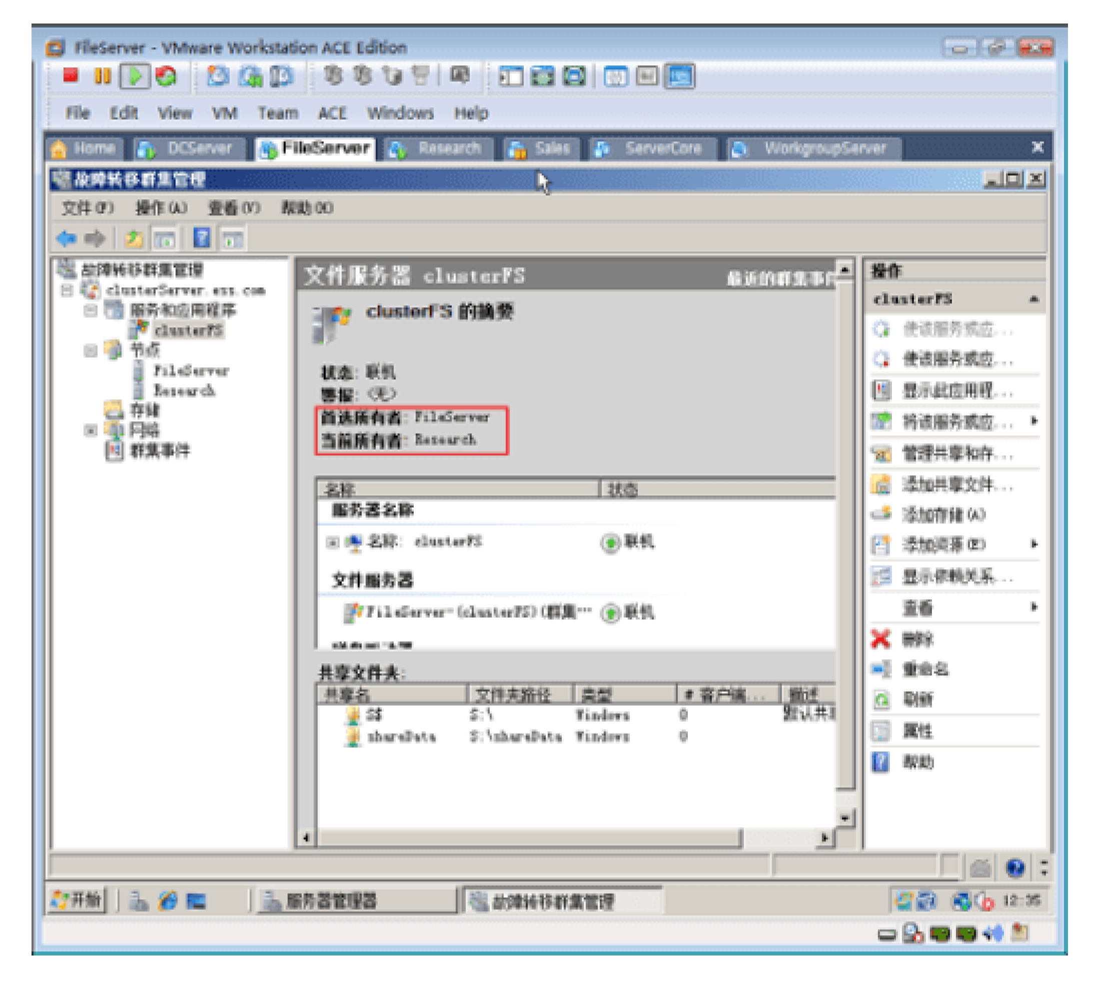


图 15-110　移动完成

15.7.5　配置首选所有者

可以指定某个程序或服务的首选所有者以及故障转移参数。

① 如图 15-111 所示，右击 clusterFS，在弹出的快捷菜单中选择“属性”命令。

② 如图 15-112 所示，在“clusterFS 属性”对话框的“常规”选项卡中，可以指定首选所有者或单击“上移”、“下移”按钮调整顺序。

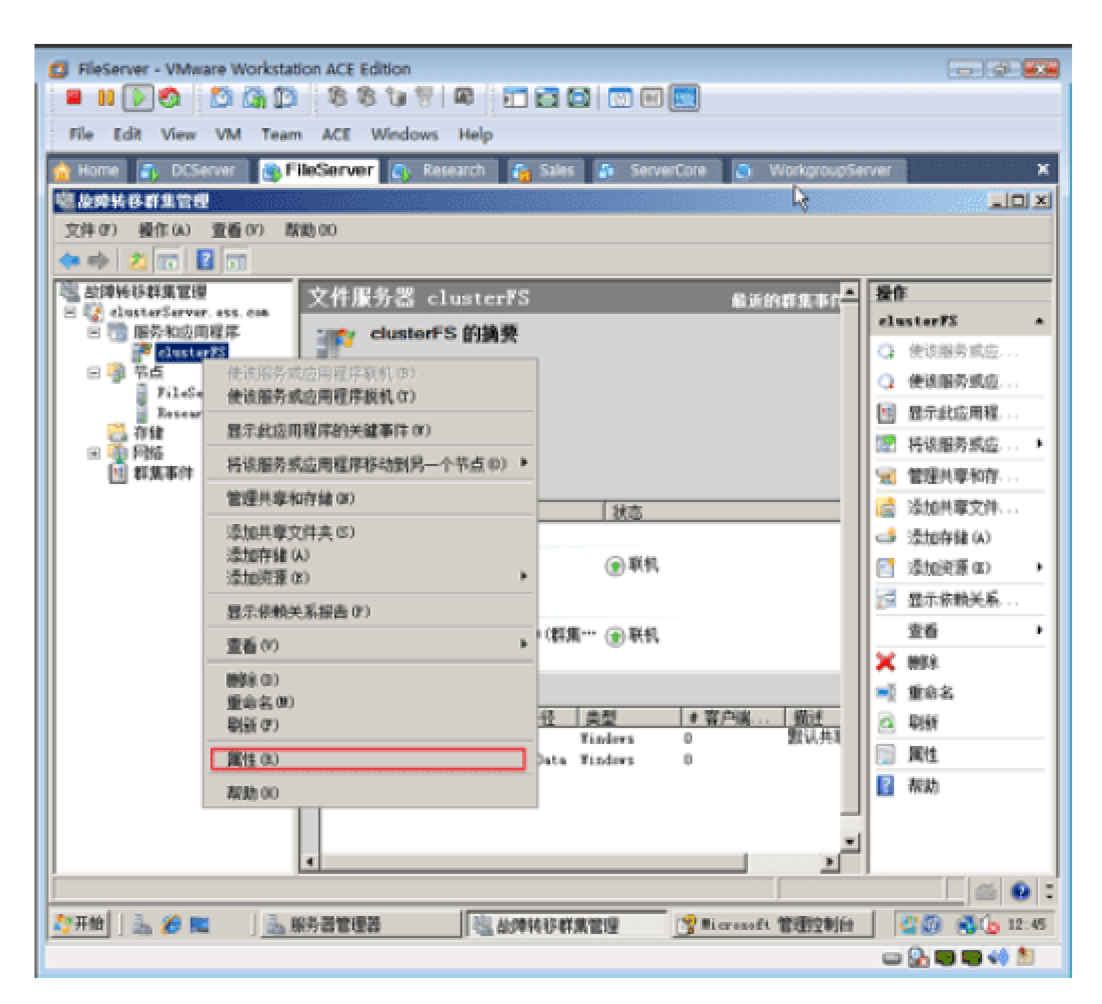


图 15-111　配置属性

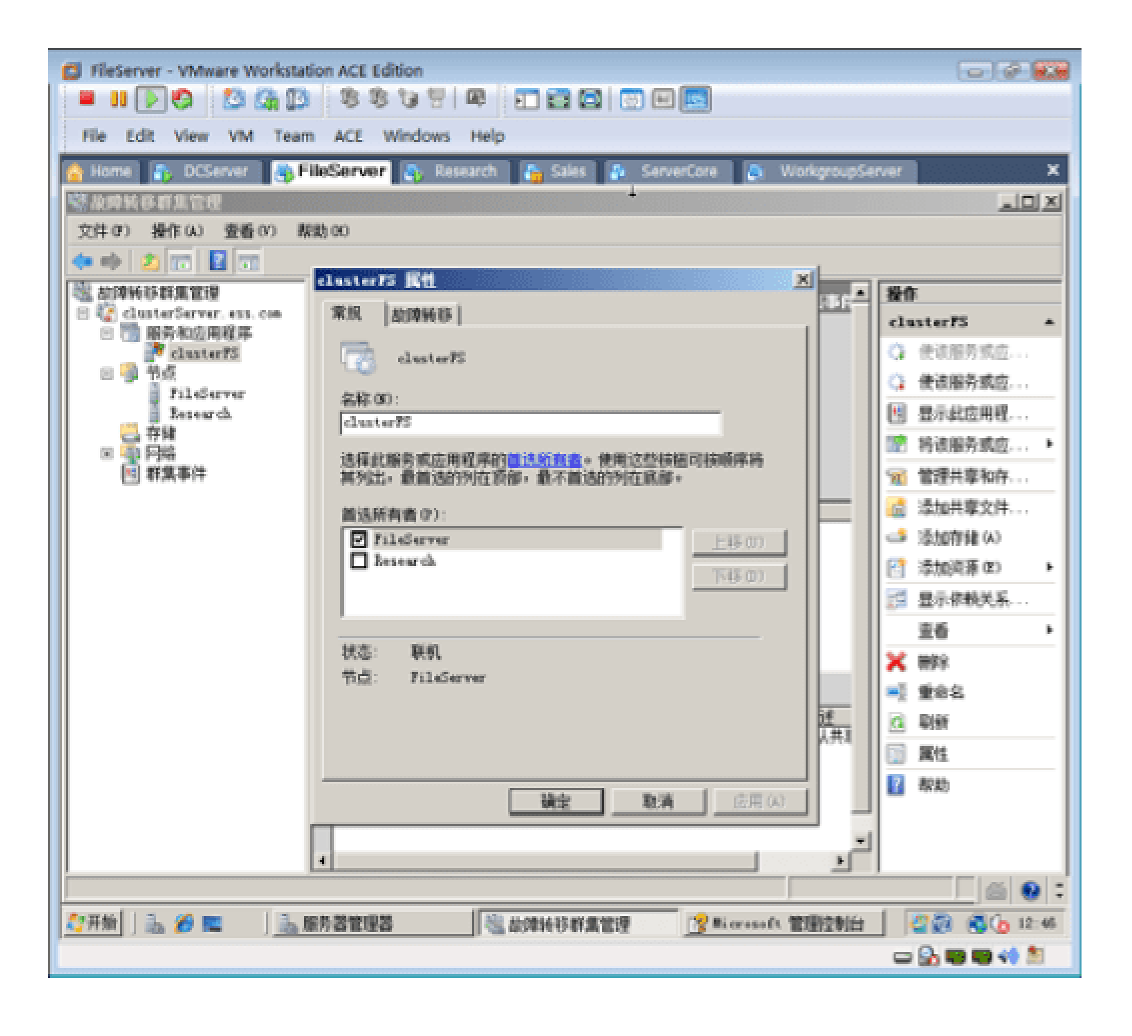


图 15-112　确定首选的所有者

③ 如图 15-113 所示，在“故障转移”选项卡中，如图中所选，在 6 小时内出现两次故障将会进行故障转移。如果选中“允许故障回复”单选按钮并选中“立即”单选按钮，当首选的所有者可用时将会立即回复到首选节点。

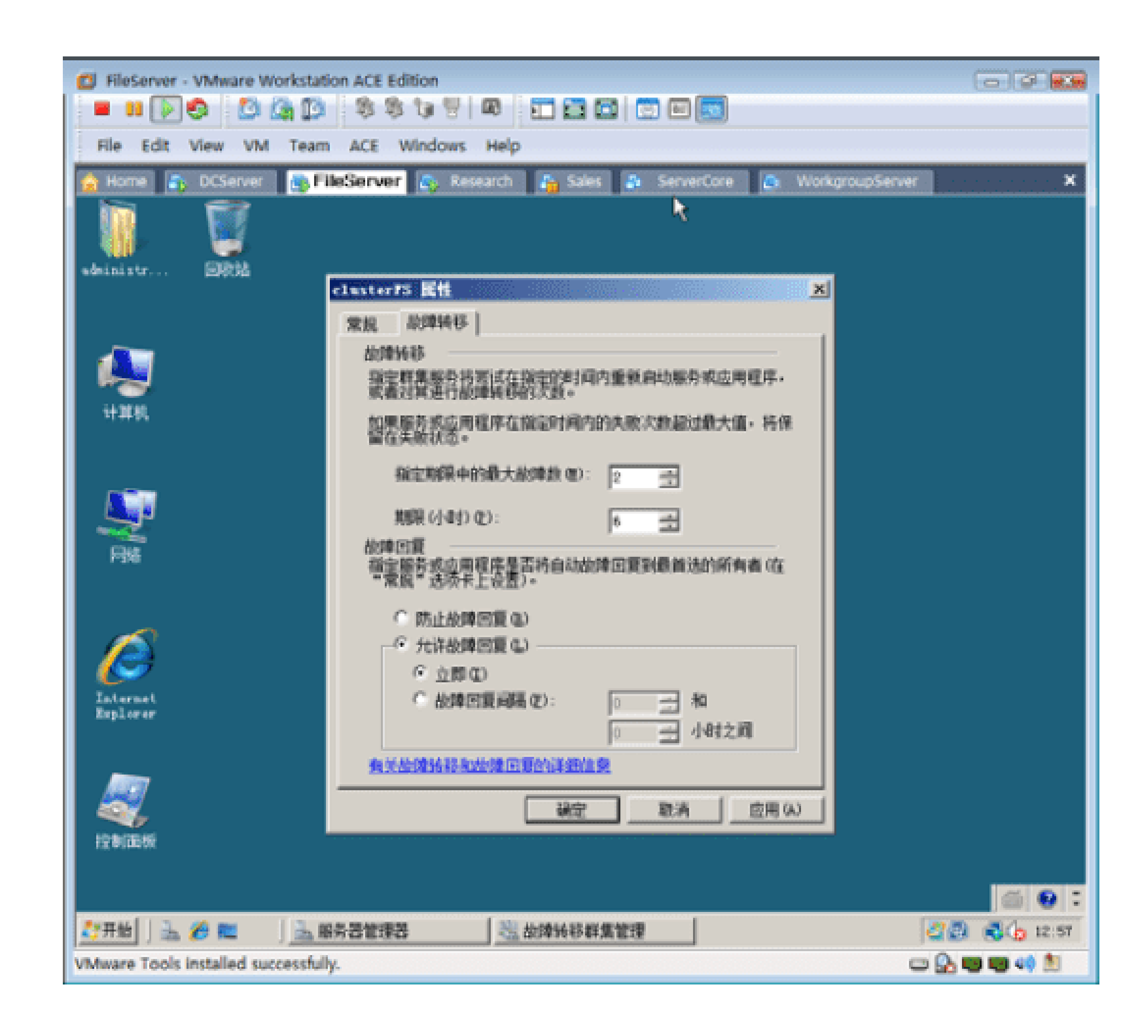
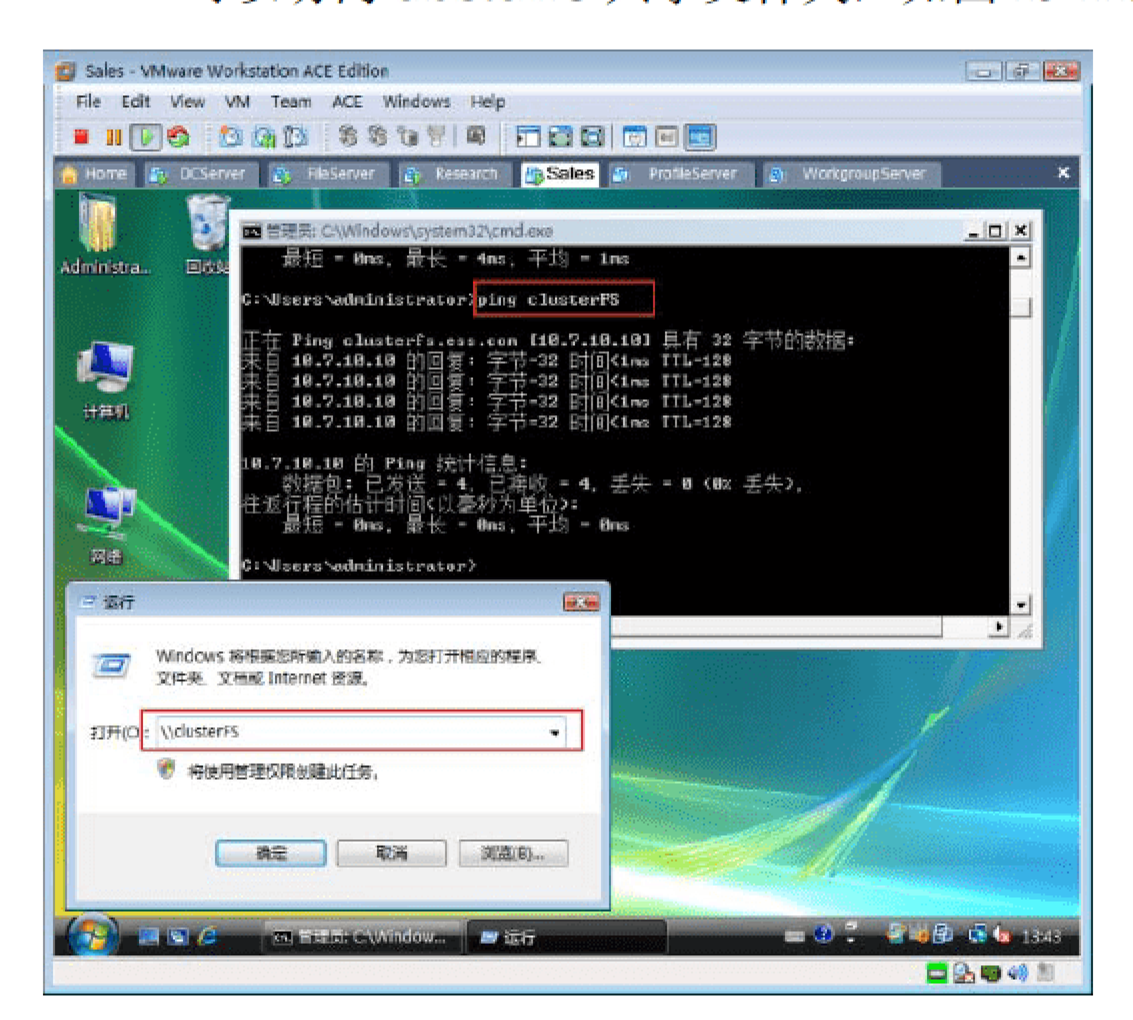


图 15-113　设置故障切换参数

15.7.6　测试文件服务器高可用

① 如图 15-114 所示，在 Sales 计算机上，输入 ping clusterFS，可以看到能够解析到 10.7.10.10 地址。

② 在 Sales 计算机上，选择“开始”→“运行”命令，在出现的“运行”对话框中输入\\clusterFS，可以访问 clusterFS 共享文件夹，如图 15-115 所示。



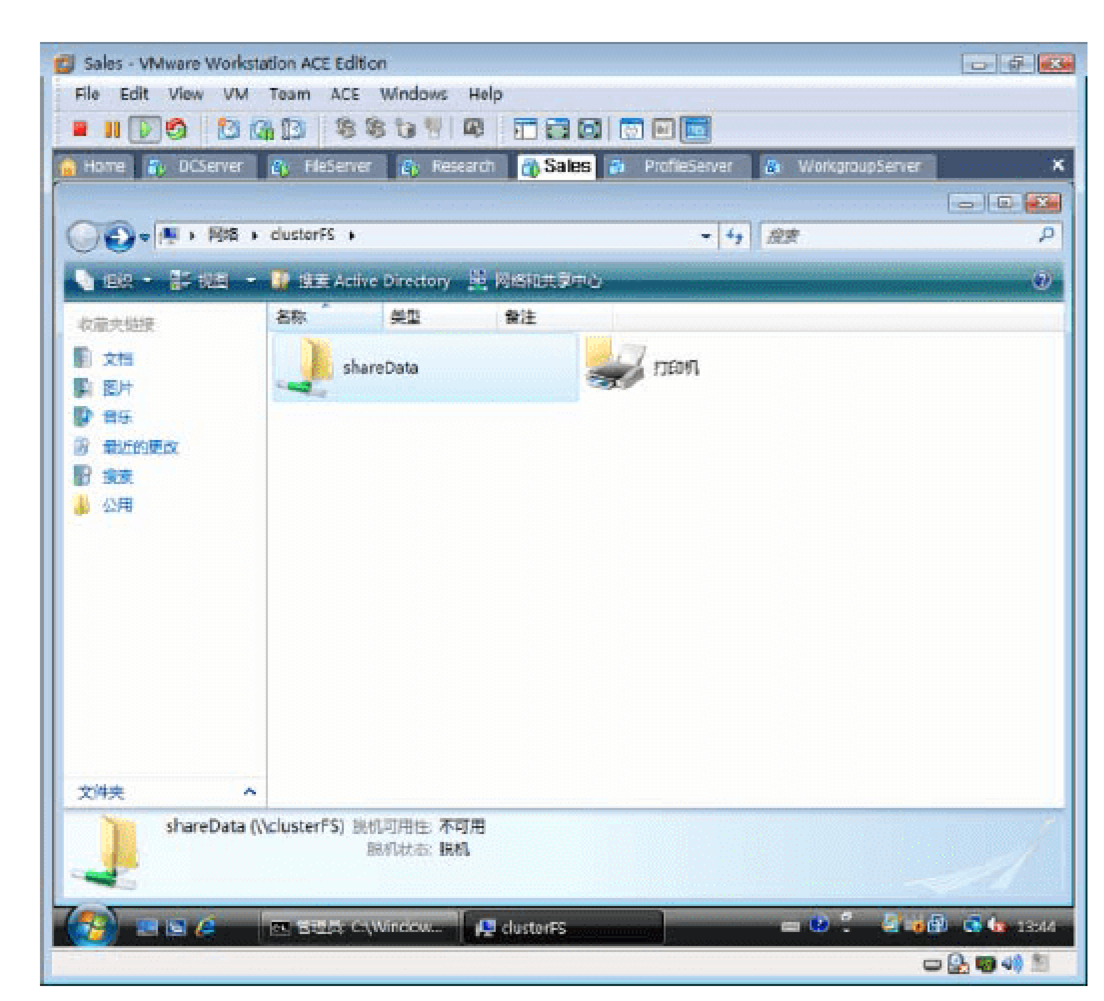


图 15-114　ping 文件服务器 IP 地址　　　　图 15-115　访问共享文件夹

③ 如图 15-116 所示，单击■按钮，关闭 FileServer，模拟 FileServer 服务器故障。

④ 如图 15-117 所示，在 Sales 计算机上，访问 clusterFS，发现照样可以访问。

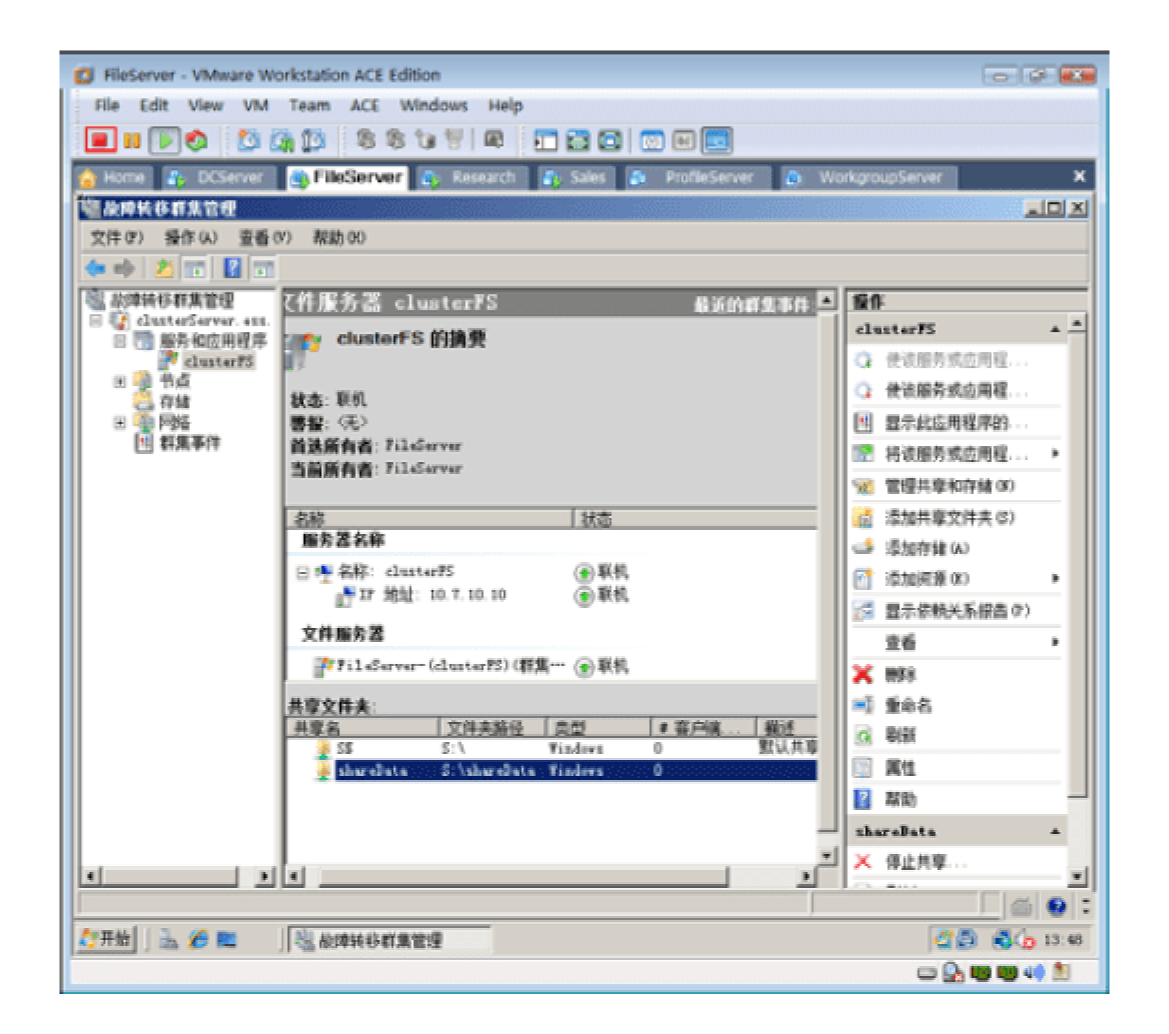



图 15-116　关闭一个节点

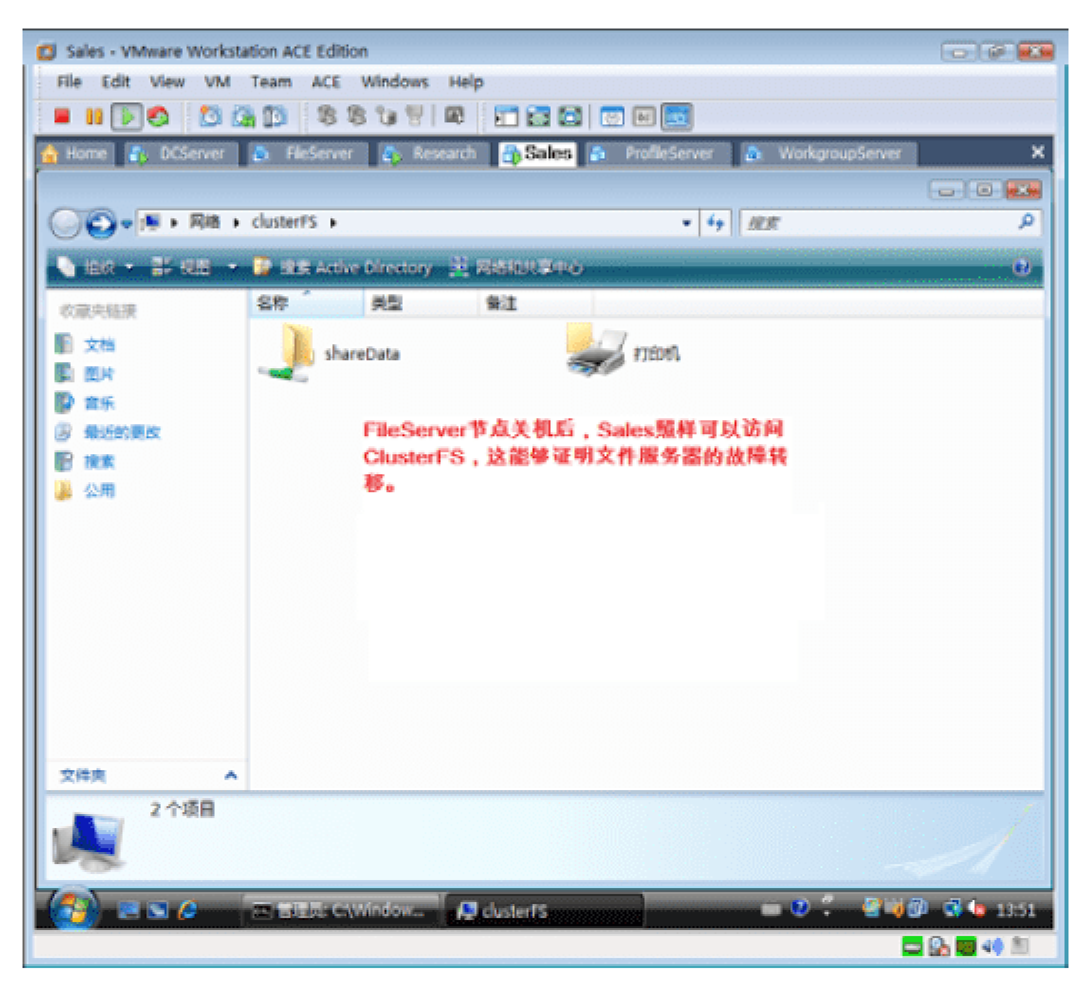


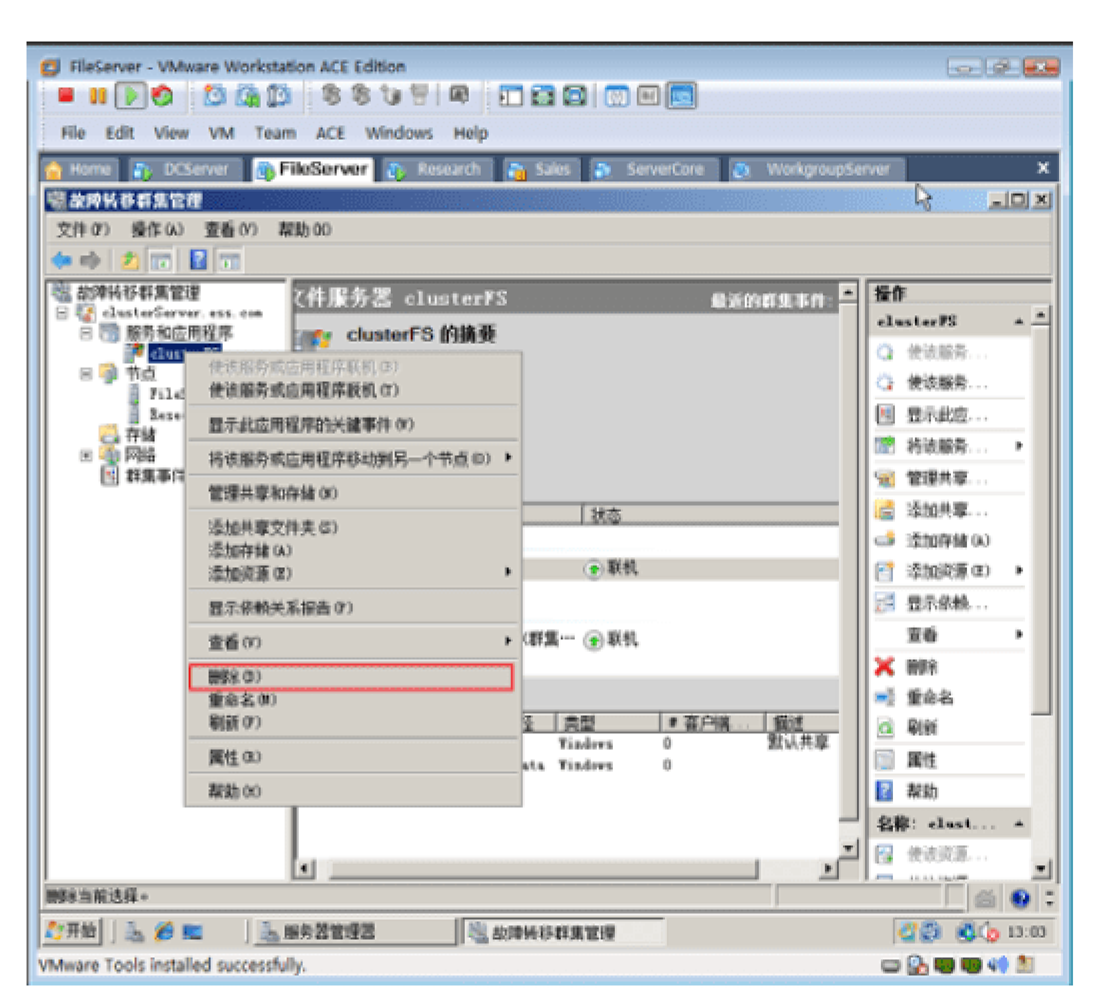
图 15-117　客户端照样可以访问共享资源

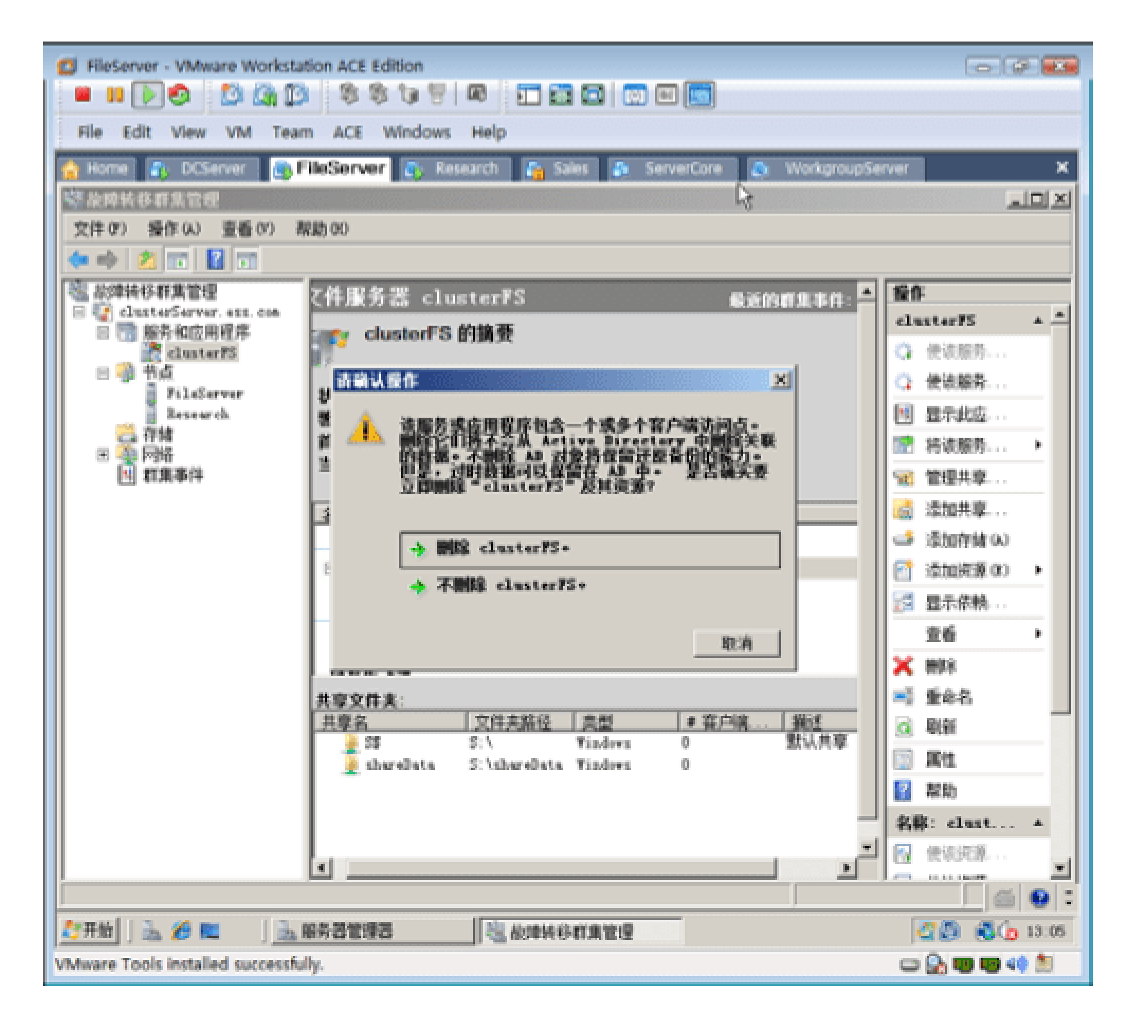
15.7.7　删除群集中的服务和应用程序

可以删除群集中的服务和应用程序。

① 如图 15-118 所示，右击 clusterFS，在弹出的快捷菜单中选择“删除”命令。

② 如图 15-119 所示，在出现的“请删除操作”对话框中，单击“删除 clusterFS”按钮。


图 15-118　删除应用


图 15-119　确认删除

③ 如图 15-120 所示，可以看到群集中不存在任何服务和应用程序。

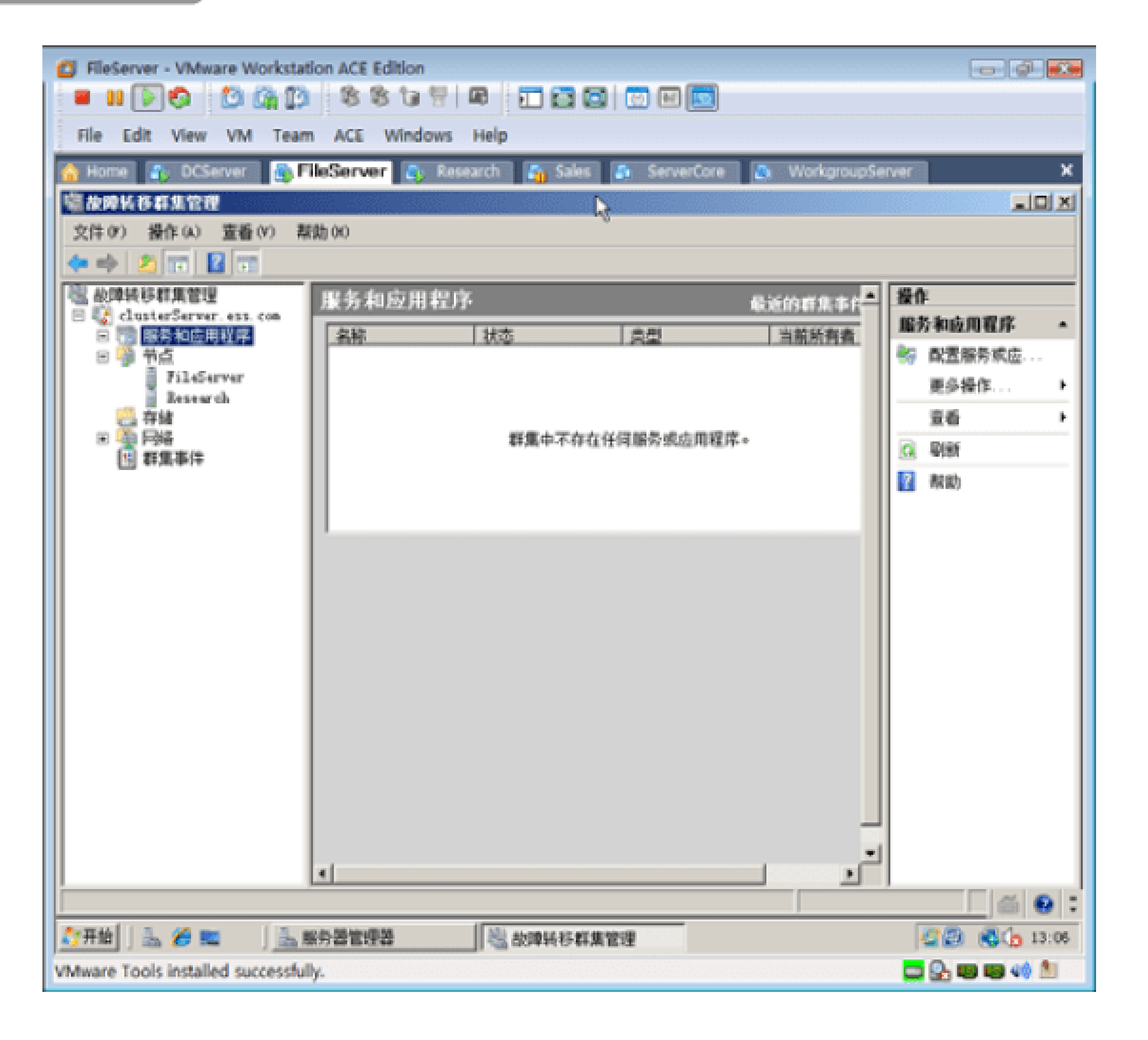


图 15-120　删除应用程序后